Manual de la Resiliencia

Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI

Alejandro Corletti Estrada
acorletti@darFe.es

Con los especiales aportes de:
General de División **Evergisto de Vergara**

Fundación UAX

UAX
UNIVERSIDAD ALFONSO X EL SABIO

"Manual de la Resiliencia"

(Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)

Madrid, octubre de 2020

RPI (Madrid): **M-006284/2020**

ISBN: 978-84-09-24465-2

Alejandro Corletti Estrada

(acorletti@DarFe.es - acorletti@hotmail.com)

www.darFe.es

Con los especiales aportes de:

General de División **Evergisto de Vergara**.

Agradecimientos:

Deseo agradecer especialmente el apoyo recibido por la Universidad Alfonso X El Sabio y su Fundación para la publicación de este libro.

**"Resiliencia no es capacidad de recuperación,
sino la certeza en recuperarse"**

Alejandro Corletti

**"Lo crítico es la INFORMACIÓN...
no las infraestructuras"**

Alejandro Corletti

Índice

1. Introducción

Nuestras infraestructuras de red y TI se nos están haciendo cada vez más "pesadas".

En los últimos años, día a día se va incrementando el nivel de actualizaciones, parches, dispositivos de seguridad, de detección, de monitorización, de prevención y detección de ataques, de antivirus, antiDDoS, antispam, antiphishing, anti…..

Llevando una vez más la seguridad informática al terreno militar, esto me hace acordar a las campañas de los grandes ejércitos de la historia, donde en virtud de los miles de combatientes, necesitaban una cantidad generalmente superior de infraestructura logística, de apoyo, de seguridad en sus puntos de conquista, de salvaguarda de sus fronteras y flancos, de fábricas y almacenes de material, de medios de transporte, etc. Me atrevería a afirmar que la totalidad de estos casos sucumbieron pues no podían soportar esta carga colateral a la acción de guerra en sí. Si se analiza la historia militar, detrás de todos ellos hubo verdaderos estrategas militares, pero su ambición los llevó a los límites del concepto de "seguridad" y fueron siendo derrotados pues no fueron capaces de mantener estas enormes infraestructuras de guerra.

Hoy nuestras infraestructuras de red y TI se me presentan como algo similar. Nos encontramos batallando en esta Ciberguerra sobre un escenario sin fronteras, obligados a exponer cada vez más nuestros recursos, incorporando nuevos elementos, aplicaciones, protocolos de comunicaciones, información que en muchos casos no llegamos a conocer a fondo pues no damos abasto, dejando con ello cada vez más potenciales amenazas.

El Ciber enemigo opera como si fuera "guerrilla" u organizaciones mafiosas. No es un enemigo convencional, no le aplica ninguna de las leyes de esta guerra (*leyes y regulaciones nacionales y/o internacionales*). Nos ataca con "golpes de mano" precisos, no da la cara, tiene organización celular, está al margen de la ley, tiene muy fácil las medidas de velo y engaño, de enmascaramiento, de evasión y escape.

Nuestra estrategia de "Ciberdefensa" no puede seguir siendo la convencional o clásica, debemos operar dentro de la ley con: nuevos conceptos, nuevas metodologías, nuevos desafíos.

No voy a profundizar en esta introducción sobre conceptos que vengo presentando desde hace años, sólo los menciono brevemente:

- Conceptos ya difundidos:
  - ➢ Defensa en profundidad y en altura.
  - ➢ Dinámica de la defensa.
  - ➢ De "Proteger y proceder" a "Seguir y perseguir" (RFC-1244)
  - ➢ Ciber operación de Acción retardante.
- Nuevos conceptos y desafíos:
  - ➢ Compartimentación de redes (la familia IEEE-802.x).
    - *Reducir superficie de ataque.*
    - *Arquitectura de red de confianza cero.*
    - *Organización por tecnologías.*
    - *Granularidad.*
    - *Exfiltración de datos.*
    - *Gestión de actualizaciones.*
    - *Capacidad de reacción.*
  - ➢ Ruido en la red.
  - ➢ Virtualización (de host y de redes).
  - ➢ Delegación y segregación de responsabilidades y funciones.
  - ➢ Contra inteligencia.
  - ➢ Juegos de ciberguerra.

Hoy sumaremos a todos estos, el tema de la "Resiliencia" tratándola de forma detallada y desde sus diferentes puntos de vista, llegando a desarrollar una metodología o guía que nos pueda ser de utilidad desde el punto de vista técnico y para la operación del día a día en nuestras redes y sistemas de TI.

2. Lo crítico es la "Información"… no las Infraestructuras.

Deseo comenzar el libro con este tema pues estoy totalmente en desacuerdo con la postura que están tomando Instituciones y Estados al respecto, centrando la atención incorrectamente en la "materia" y no en lo "inmaterial". Reconozco que es muy difícil con nuestras mentes tan preparadas durante milenios a pensar así, pero el siglo XXI se nos está viniendo encima con cambios muy substanciales e innovadores, que para peor suerte son tan acelerados que nos llevan a una vorágine difícil de parar y reencauzar, sobre todo nuestras líneas de pensamiento. Esto no es trivial, es la causa raíz desde donde se debe enfrentar el problema.

Es momento que lo hagamos, debemos decir basta a lo físico y empezar a movernos en el mundo virtual, ese es el desafío principal para nuestras redes y sistemas de TI. Lo físico son las infraestructuras, lo virtual es la información, hoy debemos jugar nuestro combate.

A lo largo de este capítulo, se presentan una serie de planteos que intentan llevarnos a la reflexión sobre el rumbo de los acontecimientos, regulaciones y medidas que se están adoptando acerca de este quinto dominio que militarmente ya ha sido reconocido como "**Ciberespacio**" y que a juicio del autor, nos está llevando a tratar el problema desde el punto de vista "físico", siendo que este nuevo escenario, todos acuerdan en que es "**virtual**", por lo que es necesario replantearnos la forma de abordarlo pues, así como el aire no se puede detener con una red por ser intangible, tampoco puede detenerse un "ciberataque" con murallas o protección de infraestructuras, debe detenerse con medidas lógicas, configuraciones adecuadas, mentes preparadas y concienciadas, innovación, procedimientos, cuidado, protección y actualizaciones de la información, medidas de inteligencia y contrainteligencia, respuestas y acciones rápidas, etc. Nada de ello guarda relación con la parte física del problema, todo ello va orientado al tesoro final que es la "**Información**".

Sin lugar a dudas la raíz del problema es la "Información", no la "Infraestructura" que la sustenta, entonces: ¿por qué el punto de partida se está enfocando en las "Infraestructuras críticas?

2.1. Las regulaciones.

Reflexiones iniciales:

El poder del siglo XXI se llama "Información".

El quinto escenario militar "Ciberespacio" tiene como límites la "Información"

El tesoro es la "Información", no la infraestructura que la sustenta.

(*No perdamos el norte sobre lo que hay que proteger*).

Cualquier familia que guarde las joyas de sus antecesores en una caja fuerte, tiene muy claro que lo crítico no es la caja fuerte, sino el tesoro que guarda dentro. Es natural que oculte la ubicación de la misma, la tape con un cuadro, no le diga a nadie dónde está. Podríamos acordar que es lógico que tome medidas físicas de protección, pero no tiene la menor duda que lo que vales son sus joyas, no la periferia.

La cultura que se está creando sobre "**Ciberseguridad**" nos está llevando a tergiversar ideas sobre lo importante y lo trascendente, y esto no es un buen punto de partida.

Analicemos la situación desde el punto de vista de la Unión Europea (UE).

En junio de 2004, el Consejo Europeo solicitó la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas.

El 17 de noviembre de 2005, la Comisión adoptó el Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas.

En diciembre de 2005, el Consejo de Justicia y Asuntos de Interior pidió a la Comisión que elaborara una propuesta para un programa europeo de protección de las infraestructuras críticas (el **PEPIC**).

El 8 de diciembre de 2008 se publica la Directiva **2008/114/CE** del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

En su artículo 2 Definiciones, expresa:

A efectos de la presente Directiva, se entenderá por:

a) *«infraestructura crítica», el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;*

b) *«infraestructura crítica europea» o «ICE»… idem. situada en los Estados miembros.*

En España, siguiendo esta línea de la UE; se publica la **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

El Título I dedica un artículo a la figura del Catálogo Nacional de Infraestructuras Estratégicas. El Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, y crea el Centro Nacional para la Protección de las Infraestructuras Críticas (**CNPIC**), y el Título IV está consagrado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

No merece la pena seguir detallando normativas, la intención de los párrafos anteriores era solamente presentar la secuencia de cómo se fue avanzando en Europa sobre el tema de Ciberdefensa y remarcar que el concepto base de todo esto fue siempre "**Infraestructuras críticas**", concepto que no comparto del todo.

Sin embargo, hasta la misma administración española, en este aspecto presenta una cierta incoherencia, pues como veremos más adelante, la metodología de análisis de riesgo **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) cuya autoría es del Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC) del Gobierno de España, en su punto 2.1 "Activos esenciales" expone:

"En un sistema de información hay 2 cosas esenciales:

— la información que se maneja y

— los servicios que prestan.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema".

Sobre estos "activos esenciales" se da inicio a toda la metodología de análisis de riesgo, que es el punto de partida más importante en una estrategia de Ciberseguridad. Uno de los aspectos que considero más importantes de esta metodología es que basa todo su análisis, justamente en la información y los servicios que esta presta a la organización, y con este pilar inicial va desarrollando todo el resto del estudio.

Volviendo al inicio de este texto, considero que lo que define al Ciberespacio no guarda relación con infraestructuras, sino con "Información".

Cuando hablamos de "Información", por supuesto que desde el punto de vista de Ciberdefensa debemos comenzar por la que consideramos **crítica**. Justamente este punto de partida, no está considerado por la **Ley 8/2011**.

El Artículo 15 de la misma. "Seguridad de las comunicaciones", es el único que al menos hace referencia a este tema

*"2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los **datos** sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.*

*3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su **confidencialidad**, **integridad** y **disponibilidad**, según el nivel de clasificación que les sea asignado."*

… pero en ninguna de sus definiciones menciona que es "Información crítica", aspecto que considero una seria omisión.

Aunque estoy centrando este texto en España y la UE, no quiere decir que esté limitado a esta región, me atrevería a afirmar que casi todo Latinoamérica está enfrentando este tema de forma similar.

En el punto 3 del párrafo anterior de este artículo 15, he remarcado intencionadamente en negrita **confidencialidad**, **integridad** y **disponibilidad**. Todo aquel que lleve años en Seguridad informática,

seguramente tiene muy presente una palabra que vengo remarcando desde hace mucho tiempo "**ACIDA**".

A: Autenticación (y si queréis también "Accesos").

C: Confidencialidad.

I: Integridad.

D: Disponibilidad.

A: Accounting (o trazabilidad).

Al no considerar la "Información" como punto de partida, sino las estructuras, prestemos atención que esta Ley no considera "Autenticación", ni "Trazabilidad" como pieza clave de Ciberdefensa.

Más adelante avanzaremos en detalle sobre estos conceptos, pero por ahora quedémonos con dos ideas:

No estamos definiendo, ni considerando la idea de "Información Crítica".

Sobre la misma, no estamos definiendo, ni considerando "Autenticación", ni "Trazabilidad".

Pongamos un ejemplo:

Todas las oficinas de la Administración de la Seguridad Social de España, gestionan los datos de los cuarenta y cuatro millones de españoles, estas son la "puerta de entrada" de, por ejemplo, mis datos jubilatorios. Estos datos que son "mi vida laboral" para mí sin lugar a dudas son "críticos", estimo que para todo trabajador español también lo es, aunque algunos desearían que no sean tan precisos como de verdad lo son…

Casi, casi, aseguraría que cada una de esas oficinas no tienen las mismas medidas de "Ciberdefensa" que el Centro Criptológico Nacional… pero allí están **¡**mis datos jubilatorios**!**, desde allí viajan a una base de datos central y espero que sobre la misma se estén adoptando las adecuadas medidas de respaldo y recuperación. Pero ¿Esta Ley no está contemplando que alguien vele por los "accesos, autenticación y trazabilidad de mi jubilación?... Es decir, si alguien logra violar las medidas de esta oficina que está en un pueblo perdido de España, compromete la terminal de ese empleado y desde allí lanza una nueva versión de "Wannacry" que criptografía toda la base de datos, y como no

hay mayor control de Accesos, también borra los backups. Dicho sea de paso, como la "trazabilidad" tampoco está contemplada, una vez que borre sus rastros, tampoco podremos saber quien fue… se perdieron todos los datos de la seguridad social de los españoles (*roguemos que no sea cerca de Navidad, pues no se sabría a quien, ni cuanto pagar su pensión, ni su paga extra… ¡felices fiestas España!).*

¿Cómo podríamos reconstruir esta historia de años de aportes (o no), de importes, de vida laboral, familiar, etc.?

¿Qué sucedería si para de criptografiarla, se pidiera una importante suma de euros, o tal vez una amnistía política, o la retirada de tropas de otro país?, ¿Cedería el Gobierno? ¿Qué harían todos los jubilados ante una Navidad sin paga?, ¿se consideraría un Ciberataque?

Tal vez lo mismo podríamos pensar sobre el registro nacional de las personas, los datos catastrales, nuestras fichas médicas, los registros notariales, los padrones electorales, los legajos de estudios del Ministerio de Educación, los antecedentes penales, las bases de datos judiciales… podríamos seguir varias página más. ¿Serán Información Crítica para España, o no?... es probable que nunca lo sepamos, pues esta ley no lo tuvo en cuenta en su punto de partida, como "Información Crítica", su máxima preocupación son las "Infraestructuras críticas".

A titulo de experiencia personal, voy a confesar que durante una breve estancia, estuve alojado en la Unidad de Cuidados Intensivos (UCI) de un gran hospital de España (*pongo de manifiesto mi más grande agradecimiento y felicitaciones al sistema sanitario de este país, pues de verdad es excelente*). Como no podía ser de otra manera, me aburría de no poder moverme, al tercer día, cuando ya me sentía más o menos bien (y aburrido), alguien cometió el error de traerme mi portátil Macintoch, dando la casualidad que en la mesa de noche de la UCI hay teléfono IP. Sin poder resistirme, desconecté el cable del teléfono y me conecté a esa línea…. Pude acceder a TODA la información de ese hospital. Como colaboro con "el lado del bien", me limité a informar el hecho a los responsables informáticos del hospital, pero y ¿si jugara "del lado del mal"?...

Conozco el detalle de algunas instituciones / administraciones que figuran en el catálogo de "infraestructuras Críticas" y, sé con certeza, que hay datos almacenados en "la nube", otras por ejemplo, (*y muy*

conocidas) emplean aceleradores de contenidos del tipo "Akamai" lo que implica que la "Información" pasa por zonas que están fuera de su responsabilidad. Es decir, la "infraestructura" seguramente cumple con todo los legislado, pero su "información" tal vez presente alguna debilidad… o tal vez no.

Una infraestructura, se la puede resumir en un conjunto de hardware (de red y TI) y software (sistemas operativos, aplicaciones y bases de datos). A medida que se interconectan, configuran y prueban, los mismos van entrando en producción y desempeñando su rol sobre la base de los servicios que deben ofrecer. En definitiva esta es la parte menos problemática, pues si sufrieran cualquier tipo de incidente, natural o artificial, los mismos se reponen o se reinstalan y el problema, con sus más y sus menos, queda resuelto en un tiempo aceptable o no, en la medida que tengamos bien implantados nuestros planes de recuperación de desastres y/o planes de continuidad de negocio. Estos mismos planes se complican a la hora de entrar en juego la "Información" que a lo largo de los años se procesa en estas infraestructuras. Cualquier administrador de sistemas sabe en carne propia que un sistema recién implantado, si falla es un mal menor, si lleva años trabajando, el tema es bastante más complicado.

2.2. Lo crítico está en la Información.

Desde un punto de vista militar, a lo largo de la historia, se fueron definiendo escenarios o dominios militares, el primero fue "tierra", luego "agua", "aire", el siglo pasado se incorporó el "espacio", y este siglo el "ciberespacio" se estableció de común acuerdo mundial como el quinto escenario militar. Cabe mencionar que ya se está hablando de un sexto dominio que se trata del de "opinión" y es el tipo de guerra orientada a la opinión pública y cómo, de forma dirigida, se pueden generar tendencias y comportamientos. Este fenómeno se está tratando técnicamente desde hace años, se lo denomina "CROWD" (*multitudes*), no solo por seguridad, sino por marketing, tendencias, I+D, etcétera, y a su vez están potenciados por herramientas o software muy poderoso que está

disponible con total facilidad en la red. Recordemos las últimas y controvertidas elecciones electorales de los EEUU de Norteamérica.

La definición de los cuatro primeros dominios es sencilla, pues se trata de espacios físicos (tierra, mar, aire y el espacio a mayor altura), pero los dos que siguen son "no tangibles", más específicamente se los denomina "escenarios virtuales". No son reales, son intangibles. Concretamente lo que define al "Ciberespacio" es la Información (*nuevamente, no son las infraestructuras*), esta información debidamente dirigida a las "mentes" crea este sexto escenario de la "opinión".

Tengamos en cuenta que la información solo se puede tratar en dos estados:

- Almacenada.
- Tránsito.

De estos estados surgen las cuatro operaciones básicas sobre la información, estos son los pilares sobre los cuáles, al igual que las cuatro operaciones básicas de matemáticas (+ - x %) se pueden construir varios cuatrimestres de estudio Universitario. Estos son:

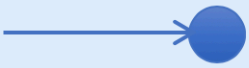
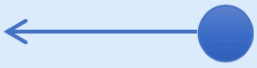
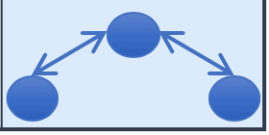
Almacenada	**Inserción / modificación**	
	Obtención / Extracción	
Tránsito	**Escucha**	
	Interceptación / Triangulación	

Tabla1: proceso información

Para poder realizar estas operaciones básicas, o combinación de ellas de forma no autorizada (sea crítica, o no) ahora sí, dentro de una "Infraestructura" de redes y sistemas, solamente existen cuatro métodos:

- Inteligencia sobre información dispersa.
- Intrusión (interior o exterior).
- Infección.
- Ingeniería social (que puede aplicar a las anteriores).

Un concepto fundamental de este nuevo "Ciberespacio" es que sin ser físico, puede causar efectos sobre la "tierra, mar, aire o espacio". Esto es un hecho inédito que me hace acordar muchísimo a cómo la "mente" de una persona puede desencadenar efectos físicos sobre el cuerpo de la misma (*imaginémonos y concentrémonos un rato que estamos masticando un limón… pensemos en su forma, color, tamaño, frescura, sabor, jugo …. ¿a que tienes más saliva en la boca?).* Lo que acabamos de hacer es ir procesando en nuestra mente, esa "Información" que tenemos almacenada respecto a lo que es un limón … pero el limón no está, sin embargo esa "Información" totalmente intangible, generó un efecto físico. Lo mismo puede realizarse, y de hecho ya lo hemos visto, con un ciberataque a una central eléctrica, un sistema de control, un movimiento bancario, un enlace de cable fibra óptica o radio enlace, la apertura de una puerta, una cámara de video, etc. Es decir, operando sobre la "Información" que circula a través de redes, hasta un dispositivo físico y alterando deliberadamente la "Información" con la que este funciona, se logra el efecto físico deseado, pero, una vez más tengamos en cuenta que SIEMPRE se trabajó sobre la "Información" de esas "Infraestructuras" para lograr el efecto final. La infraestructura fue el resultado, no el foco del ataque. Si deseara haber evitado el ataque, lo que debería haberse mantenido "íntegro" es la "Información", pues sin alterar la misma, no hubiese tenido efecto el ataque.

Algo que hace años me asombró mucho, fue que las Centrales Nucleares no admitían desarrollos de software en su funcionamiento, todo tipo de proceso debía diseñarse, probarse y una vez que se garantizaba al cien por ciento su régimen de funcionamiento, se imprimía en una placa de hardware, ni siquiera "firmware" que es re escribible. Hoy no sé si seguirá siendo así, pero deseo presentar el concepto de fondo: todo esto se hacía así para evitar que de alguna forma

(*intencionada, o no*) pudiera alterarse la "Información" que debía procesarse en cada paso o control del funcionamiento de la Central, NO existía posibilidad de alterar ese sistema, pues su información y flujo dejaba de ser intangible, estaba impresa en una placa. En definitiva no deja de ser como esas viejas tarjetas perforadas en la que pasaba o no la luz, o un medio mecánico. Si el agujero no está, pues la luz no pasa y listo. En estos casos podría aceptar que se hable de "Infraestructuras", pues para lanzar un ataque, hay que hacerlo de forma física, llegar a la placa impresa y reemplazarla o soldarle otro circuito, o hacer otro agujero nuevo en la tarjeta perforada.

Todos sabemos con absoluta certeza que hoy en día no hace ninguna falta levantarse de un ordenador en un extremo del globo, para lanzar un ataque con toda la sofisticación que se desee sobre cualquier sistema o red, pero en definitiva:

¿Qué es lo que se busca atacar?

En TODO ataque lo que se está "**agregando** – **borrando** o **modificando**" es la "Información". Si la red cae, es porque alguien modificó la "Información" de configuración del router, switch o servidor de red, tirándolo abajo, cambiando sus rutas, colapsando un vínculo, de sincronizándolo, etc. Si un sistema se cae y no es por fallo, es porque alguien lo alteró, modificando su "Información" al infectarlo, borrarlo, sabotearlo. Si alguien accede a una base de datos para hacer cualquier tipo de acto vandálico, su finalidad no es sobre el motor de la misma (Oracle SQLServer, Mysql, posgres, etc.) su objetivo será la "Información" que esta almacena. Podríamos seguir así con un servidor de correo, web, archivos, centrales de telefonía, etc… La finalidad de cualquier intruso será la "Información" de esa empresa, organización, red o sistema.

La infraestructura de la organización o empresa será el efecto final que ocasione este dominio intangible liderado absolutamente por la "Información" que ha sido mal salvaguardada.

2.3. La raíz del problema.

La razón de esta tergiversación de prioridades, entre lo que de verdad es crítico y lo que no lo es (o lo es menos), tal vez esté en que el concepto de "**Ciberdefensa**". Como su propia palabra lo indica, a nivel gubernamental o político se haya asociado a las diferentes jerarquías de "Defensa" que poseen los estados (*Ministerios, Fuerzas armadas y de seguridad, etc*.). La historia militar que es milenaria, y su experiencia en el campo de batalla es lo suficientemente amplia como para que nos tentemos de buscar allí la solución a este nuevo problema al que nos enfrentamos.

Cuando se unen:

- **el tiempo milenario**.

y

- **la experiencia muy afianzada**.

A veces no es la mejor combinación, y arrastra una inercia difícil de revertir.

La Ciberguerra rompe muchos esquemas militares excesivamente arraigados, y justamente debe combatirse con nuevas armas y metodologías que se oponen, a veces de forma radical, con la doctrina militar.

No desearía extenderme en este texto sobre conceptos que ya he desarrollado en detalle, los cuáles podéis leerlos de mi último libro "**Ciberseguridad, una estrategia Informático/Militar**" que me atrevo a citar aquí pues su descarga es gratuita desde www.darFe.es, pero sí creo que debemos reflexionar al menos sobre ciertos puntos (se detalla entre paréntesis el número de página correspondiente al mencionado libro, "Pág xx"):

> *"cada país aislado NO PUEDE HACER NADA…… ABSOLUTAMENTE NADA (así de duro)" (Pág 13).*

Esto a nivel militar es muy difícil de asumir, cuando se tata de "compartir información" más allá de las propias fronteras.

Antes de Internet el tema era radicalmente distinto por las siguientes razones (Pág 18):

> *1) Identificación del enemigo o agresor*
>
> *2) Hipótesis de conflicto*

3) Mutua Destrucción Asegurada

4) Capacidad bélica

5) Tipo de respuesta

6) Por último, el gran interrogante:

El ciberespacio ¿Es un dominio militar?

Como veremos a continuación, estos conceptos, cambian radicalmente.

El Oficial de Inteligencia de un teatro de operaciones militar en un escenario clásico es el "J2". Él es el responsable de evaluar la situación del enemigo. En una batalla convencional, el J2 despliega un gran folio sobre la pizarra que está a un costado de la mesa de operaciones, con todos los datos que presentaremos a continuación completos. Pero pensemos ahora cómo sería la misma en un escenario de "Ciberespacio". Los datos del enemigo serían (Pág 47):

- *Composición: Desconocida*
- *Disposición: Desconocida*
- *Magnitud: Desconocida*
- *Cantidad: Desconocida*
- *Capacidades: Desconocidas*
- *Experiencia: Desconocida*
- *Armamento: Desconocido*
- *Localización: En todo el mundo*
- *Movimiento: Desconocido*
- *Potencia conocida: Desconocida*
- *Identificación: Ninguna*
- *Objetivo: Desconocido*
- *Impresión: Total Desconcierto*

Así de crudo, duro y concreto... ¿De quién nos defendemos?

¿Cómo puedo pensar una defensa física (Infraestructuras) frente a semejante cambio de escenario?, el viejo orden de batalla debe modificarse radicalmente en este Ciberespacio.

Finalizando con partes del libro, en la página 48 se presenta:

> *Todo Internet se regula por una serie de recomendaciones, estos documentos que ya superan los ocho mil, son los que establecen las "pautas" (o mejores prácticas) a seguir. Uno de ellos es la RFC (Request For Comments) – 1244 (Política de seguridad), si bien ya existe una más actualizada, esta, en el punto el 2.5. propone dos estrategias de seguridad:*
>
> - *Proteger y proceder.*
> - *Seguir y perseguir.*

La primera de estas estrategias, si deseáis leer el libro o la RFC, veréis que es obsoleta y no puede ser aplicada en el Ciberespacio, nuestro objetivo es la segunda. Para "Seguir y perseguir" un Ciberincidente, no tiene el menor sentido pensar en "Infraestructuras" pues justamente NO se habla de fronteras o límites, sino de gestión y control sobre la "Información" que me facilite la libertad de acción suficiente para librar este combate de pura "Incertidumbre", la cuál solo se vence con "Información".

Este nuevo campo de batalla no se puede pensar en términos convencionales de espacio y tiempo, que son los parámetros que sustentan toda la ciencia conocida como "Física clásica" y debe ser este, el factor que ha llevado a esta tergiversación de comenzar a desarrollar una cultura de "Infraestructuras", como buena ciencia o mentalidad tangible. Bajo este concepto, se trata el problema con el método convencional que tenemos de la física clásica. Parece como que los legisladores de este nuevo Ciberespacio, no se han percatado que el corazón de la física del siglo XXI se llama "Física Cuántica" que se rige por leyes no convencionales, difíciles de comprender, por la pura incertidumbre (*recordemos los principios de* ***Heisemberg***), es el mundo de lo no tangible. Ya sabemos con total certeza, que el átomo no es el de Borg, que la luz se curva, que el espacio no es el de las tres dimensiones Euclidiano, sino el cronotrópico de **Einstein**. Las cosas ya no son lo que parecen ser y este es el nuevo escenario. No pretendamos combatir con la física clásica este nuevo escenario "cuántico", pues erraremos el camino, buscaremos electrones donde no los hay. No busquemos protones y electrones de hardware en salas, paredes y alambrados, sino que tengamos la esperanza matemática o la

probabilidad de que existan vectores de ataque sobre los intangible, sobre la "Información".

Estimo que la doctrina de Ciberdefensa, se está basando en estos pilares clásicos y convencionales, dando como resultado de ello la preparación de una batalla convencional sobre las "Infraestructuras", camino que no tiene probabilidad de éxito frente a cualquier enemigo que se esté preparando para un combate no convencional, cuyo objetivo final sin la menor duda estará puesto en nuestra "Información crítica".

Por último, con sólo remitirnos a los hechos, podemos ver en el día a día como las empresas líderes del mercado apuestan por el "poder de la Información". En estos momentos Google, Facebook, Whatsapp, apuestan por tener más y más "**Información**" que le permitan inferir o inducir tendencias (sexto escenario: "Opinión"). Estas empresas son cada vez mas poderosas pues cuentan día a día con más "Información", no lo son porque tengan más infraestructuras. Estas empresas saben que deben proteger al máximo su "Información" pues ese es su negocio.

Bajo este mismo principio es que, también ciertas empresas, que poseen la tecnología y la capacidad de explotar debidamente este tesoro de la "**Información**", han logrado cambiar el rumbo de procesos electorales, influir sobre las masas, revertir resultados, modificar ciento ochenta grados la opinión pública, obtener rescates con ataques tipo Ransomware.

Este es el nuevo escenario mundial, tanto es así que para cerrar este capítulo, dejo como reflexión final, lo que en el ámbito de Defensa se está presentando hoy como los futuros escenarios militares y que será desarrollado en detalle en el siguiente capítulo:

- Físico.
- Virtual.
- Opinión.

Es muy probable que las nuevas generaciones militares, lo estudien bajo este enfoque, no como los seis que se fueron tratando durante este texto. De mas está decir que el primer escenario es lo que quedará de: tierra, agua, aire y espacio (es decir "Infraestructuras") y los dos nuevos, el futuro, solo se refieren a "Información".

¿De verdad podemos seguir pensando en "Infraestructuras críticas"?...

¿No será mejor empezar a tener un poco de visión de futuro y apostar de una vez por todas por "**Información crítica**"?

2.4. Conclusiones finales.

Somos conscientes desde principios de este siglo que se ha puesto de manifiesto el tema de la Seguridad de las infraestructuras de redes y TI de las diferentes empresas y organizaciones, el mismo ya estaba dejando de ser un problema menor. Esta realidad, comienza a tomar envergadura a través de nuevos actores organizados en grandes redes delictivas, mafias y hasta Estados. Bajo esta nueva visión comienza a acunarse acertadamente el término de "Ciberseguridad".

En virtud de alarmas que empiezan a sonar a través de Internet, se hace evidente que la envergadura del problema, puede desencadenar en conflictos internacionales pudiendo afectar masivamente a una población entera con daños comparables a los de un conflicto armado. Bajo estos indicadores comienza a regularse el tema de cómo proteger o defender las piezas clave de un País ante este mal.

Al tratarse de un tema de Defensa nacional, como es natural la bandera la levantan las instituciones del área de "Defensa", naciendo la palabra "Ciberdefensa".

Este tipo de organizaciones, como se ha comentado son milenarias y poseen vasta experiencia, en particular sobre técnicas convencionales de operaciones. Es probable, que por esta última razón, es que se empieza a dar forma a un concepto de "Ciberdefensa" basado en "Infraestructuras".

A lo largo de este texto, se ha intentado presentar diferentes enfoques, con la intención de poner de manifiesto que lo verdaderamente "Crítico" del problema, no son las Infraestructuras, sino la "**Información**".

Este cambio de punto de partida, se ha abordado bajo las siguientes ideas:

- Poniendo de manifiesto que la joya, el verdadero tesoro, es la "Información", no la infraestructura.
- Por la omisión de "Autenticación" y "Trazabilidad" de las regulaciones.
- Por la diferencia entre lo "material" y lo "intangible".
- Por el objetivo real de un ciberataque, que se trata de la información en tránsito o almacenada.
- Por diferentes aspectos relacionados con el combate convencional, o el empleo de la Fuerza en las operaciones clásicas, y la inercia que traen las mismas.
- A través de una nueva perspectiva de los dominios militares: Físico, virtual y de opinión.
- Desde un enfoque de la ciencia "Física clásica" o "Física cuántica".
- Por último sobre la base de las grandes empresas actuales que tienen claro el "Poder de la Información".

Bajo estas diferentes perspectivas, es que se ha tratado de enfocar este nuevo paradigma de "Ciberseguridad" llevándonos a valorar lo verdaderamente trascendente de nuestras redes y sistemas, frente a lo que si bien es importante, no es la razón de ser de lo que debemos proteger. Por esa razón es que, en este texto y a juicio del autor, se aprecia que debemos reencauzar la raíz del tema, dejando de lado el concepto de "Infraestructuras Críticas" que está siendo el corazón de la "Ciberdefensa" de la mayoría de los países y regiones, para orientarnos mucho más en nuestro verdadero tesoro que es sin lugar a dudas la "Información Crítica".

Como todo conocimiento milenario y experiencia fuertemente arraigada, es extremadamente difícil de cambiar, pero si no comenzamos a hacerlo, estaremos cometiendo un error grave sobre un enemigo que sí lo tiene claro y sabrá golpearnos sobre lo que más nos duele, nuestra "Información" y no tendremos capacidad de reacción, ni de "Seguir y perseguir" pues estaremos atados a un combate convencional, esperando órdenes, cumpliendo taxativamente con las reglas del combate clásico,

limitados a fronteras y murallas, con reglas de juego que no aplican a la "Física moderna", o mejor llamarla "cuántica" que nos impone Internet hoy en día.

3. *El poder de la Información y las realidades inexistentes.*

Por el "General de División **Evergisto de Vergara"**.

Mi profesión es militar, es decir según la Real Academia Española, profeso la milicia, el arte de hacer la guerra y de disciplinar a los soldados para ella.

Una de las características de esta profesión es querer aprender de hechos que ya ocurrieron, lo cual es un error. Todas las guerras son únicas e irrepetibles, y no hay ninguna guerra parecida a la anterior. Eso ocurre porque el ambiente operacional donde se desarrolla este fenómeno social, es cambiante. Cambian los escenarios, cambian los protagonistas, cambian los medios que se usan, cambian los riesgos, cambian los peligros, cambian las ambiciones. En este escenario de cambios que involucra a la naturaleza humana, nada es lineal. Es difícil pretender hacer del empleo violento de los medios una ciencia, ya que obedece a pocos principios. **Clausewitz** sostiene en su obra "De la Guerra", que hay pocos principios que puedan científicamente aplicarse para asegurar el éxito. En esto, disiente con su contemporáneo **Jomini**. Más aún, Clausewitz es totalmente renuente a aceptar ninguno, aunque al final de su obra termina aceptando tres: el esfuerzo principal de su fuerza para obtener lo que quiere, la concentración en el lugar correcto y la rapidez para decidir y actuar, sin distraerse en cosas baladíes. La sorpresa la acepta parcialmente, porque aprecia que es más fácil de obtener en el nivel táctico que en el nivel estratégico [1].

Por eso es difícil asignar el carácter de ciencia a la guerra. Y si se trata de arte, es al menos un arte muy particular: se ejerce sobre cosas que reaccionan, y que reaccionan diferente ante el mismo estímulo según sean las circunstancias. Es difícil pensar que la guerra es ciencia, cuando los hechos no guardan estricta relación entre causa y efecto. En este fenómeno social, a una causa corresponden varios efectos, según sean

[1] Clausewitz Carl, On War, Edited and Translated by Michael Howard and Peter Paret, Princeton University Press, Ed 1976, Introductory note of Bernard Brodie, P.57

las circunstancias. Varios efectos reunidos no obedecen siempre a la misma causa. Es por eso que es difícil pensar en la guerra como una ciencia. Es lo que se denomina el pensamiento adaptativo, no lineal y complejo.

De observar la realidad surge claramente que en la historia de la humanidad, y específicamente en el fenómeno social guerra, el hombre con la tecnología se fue alejando del enfrentamiento directo. Primero se enfrentaban en lucha directa, luego con piedras y hondas, después con arcos y flechas, luego con lanzas y picas, apareció la pólvora y los mosquetes, luego los rifles, luego los cañones, la aviación después los tanques, los helicópteros, los barcos, los submarinos, los proyectiles intercontinentales y las armas de destrucción masiva. Puede verse que lo que hizo el hombre fue encontrar armas que lo alejaban del enfrentamiento directo y de la lucha cuerpo a cuerpo.

Este cambio en la naturaleza de la guerra – en el concepto de Clausewitz - el tipo de warfare en sus formas externas, dio lugar a que estas guerras se emprendieran con diferente propósito y se condujeran en cada tiempo, en forma diferente. Esta influencia de la tecnología en el cambio de la naturaleza, propósito y forma de conducir la guerra se llama en los ámbitos académicos, "Revolución en Asuntos Militares". Hay varios autores que tratan sobre el significado de esta frase, yo solamente retengo el que me fue enseñado en el **National War College** de la **Universidad de la Defensa Nacional**, Washington DC, en el año 1996.

> *Frecuentemente esta frase se refiere en el contexto de revoluciones previas: la ramificación político y social de la Revolución Francesa, los cambios tecnológicos a fines del S XIX del ferrocarril, el telégrafo, y el ánima rayada de las armas ("rifling" en inglés, de donde viene el término "rifle" -por fusil - en castellano), los cambios ocurridos entre la IGM y la IIGM como los tanques, aeronaves y submarinos, y los cambios producto de la era nuclear. Hoy en el siglo XXI bajo la frase "Revolución en Asuntos Militares" se entienden dos conceptos: uno de ellos, es el adelanto en informática, que permite avances en armas de precisión y en sistemas de computación, comando, comunicaciones, control, inteligencia e informática (**C⁴I²**); otros miran más allá de la tecnología y apuntan a los cambios sociales que tienen la potencialidad*

de cambiar las razones por las cuales se va a la guerra. Y más recientemente, la simbiosis entre delincuencia común y agresión estratégica [2].

La observación permite identificar que en la historia de las guerras, cada vez que hubo innovaciones tecnológicas, cambió la naturaleza, propósito y forma de conducir la guerra.

El progreso de las Tecnologías de Información y Comunicaciones (TICs)

El cambio tecnológico más significativo que tuvo lugar a fines del S XX fue el progreso de las Tecnologías de Información y Comunicaciones (TICs). Una misma generación fue testigo del cambio de la radio de válvulas a las de chips pasando rápidamente por los transistores, la aparición de las primeras computadoras en la argentina como las Commodore 64, hasta las laptops ultra delgadas de hoy. Desde la máquina de escribir Olivetti, las efímeras máquinas de escribir eléctricas hasta las electrónicas. La aparición de la televisión fue una conmoción, Hay muchísimos ejemplos más. Pero aquí, lo crítico es la información, no las infraestructuras, como dice el apotegma del autor del libro.

Fue así que en el ambiente militar, ya dejó de hablarse de ámbitos específicos como aire, mar y tierra. A fines del siglo XX ya se habló de espacio, y luego se agregó tímidamente la información de los ámbitos electromagnético y cibernético. Había transcurrido pocos años de iniciado el S XXI, cuando se introdujo una nueva categorización agregando un nuevo dominio a los tradicionales: la información, que incluye el espacio cibernético y el espectro electromagnético [3].

Tal como se expresa en el libro "**Percepciones son realidad**", los líderes del siglo XXI visualizan y entienden el ambiente operacional mediante la información. La información es un elemento del poder de combate de una tropa, de la misma manera que lo son el comando y control, la inteligencia, el movimiento y la maniobra, el apoyo de fuego, el

[2] Trama Gustavo, Vergara Evergisto, La naturaleza, propósito y forma de conducir la guerra desde Napoleón hasta nuestros días, texto de enseñanza inédito, para el Curso en Estrategia Militar y Conducción Superior, de la Escuela Superior de Guerra Conjunta, Argentina, año 2020, P. 11

[3] Estado Mayor Conjunto de EEUU, Joint Publication JP 3-0 Incorporating Change 1 22 Oct 2018, Ed 2018, Chapter I Fundamentals of Joint Operations, Strategic Environment, P. I-3

sostenimiento y la propia seguridad. La información es indispensable para el proceso de toma de decisiones, y su adecuada difusión y divulgación ayuda a la obtención de la victoria en muchas formas [4].

Esto adquiere más importancia con el esparcimiento de la tecnología moderna. Esta tecnología que se modifica y mejora a cada instante, ha aumentado la velocidad, el volumen y el acceso a la información. También, al mismo tiempo, es la misma tecnología que ha proporcionado medios importantes para interrumpir, manipular, distorsionar o negar información. Tan grande es la influencia de la información en la preparación del ambiente donde se va a operar y conducir las operaciones que se dice que quien controle la información puede dominar la competencia y el conflicto [5].

Por lo tanto, con el mismo énfasis con que los conductores deben dirigir sus recursos para la obtención de información que les permita decidir correctamente, también deben proteger la propia información en todos los dominios para no ser manipulados.

Aquí los investigadores se encuentran con un dilema: se aceptan las operaciones de información puramente militares, que buscan afectar al proceso de toma de decisiones del enemigo o adversario: el comando y control, la obtención de información de la inteligencia militar sobre dispositivos o intenciones del adversario, el engaño militar, la criptografía, la disuasión por medios militares, y las operaciones cibernéticas con fines militares. Estas operaciones militares se llevan a cabo en una guerra. No obstante, el dilema es una zona gris, donde se maneja y manipula información civil, pero que sirve a fines militares. Por ejemplo, alterar el funcionamiento cibernético de represas de agua, o de abastecimiento de energía eléctrica, o de funcionamiento bancario, o de tráfico de transporte aéreo, o de registros sanitarios y de salud de la población.

Hasta algunos hechos delictivos y/o criminales pueden considerarse que afectan gravemente a un adversario, por ejemplo la trasferencia de fondos bancarios, o los secuestros y actos terroristas de envergadura. Estas son operaciones que van a afectar a la población que las fuerzas

[4] US Army University Press, Perceptions are reality. Historical Cases studies of information operations in large scale combat operations, E Vertuli Mark and Loudon Bradley, Fort Leavenworth, Kansas, Ed 2018, paragraph It is all About Information, P. xii.

[5] Kaplan Fred, Dark Territory: The Secret History of Cyber War, Ed Simonand Scuster, New York, 2016, P 31.

armadas del adversario tienen que defender y se podrían definir como operaciones no militares de guerra. Afectar el comportamiento social de una población también está incluido en estas operaciones no militares de guerra y esto se logra difundiendo información errónea, falsificando información o modificando comportamientos usando las redes sociales [6].

No es intención de este escrito referirse a los aspectos militares de la información y su rol preponderante en el proceso de toma de decisiones. Este escrito pretende incursionar en una realidad potenciada actualmente, que es la percepción de la realidad a través de la información. El título de este ensayo nos lleva a la creación de escenarios que fueron creados virtualmente, pero que en realidad no existen.

El rol de la opinión pública en los conflictos

Fue a partir de la Guerra de Vietnam que la opinión pública comenzó a tener importancia en el mundo occidental, al punto que hasta llegó a influenciar la política exterior de los Estados. Alguien descubrió que la democracia era un sistema adoptado en Occidente, y que se basaba en elecciones abiertas y libres, razón por la cual si alguien ambicionaba obtener el poder todo consistía en influenciar la opinión pública con adecuada información ajustada a los intereses de quienes querían llegar al poder.

Alguien podría preguntarse acerca de algún ejemplo de historia de guerra que mostrase la importancia de la opinión pública. La guerra de Vietnam es el ejemplo más relevante. La Ofensiva de Tet de Enero de 1968 fue una operación militar gigantesca de las fuerzas de Vietnam del Norte y la guerrilla Viet Cong, ofensiva que fue derrotada por el ejército de Vietnam del Sur y las fuerzas estadounidenses. Las pérdidas norvietnamitas se contaron por miles. Fue una ofensiva que no tuvo el éxito militar esperado: el ejército de Vietnam del Sur no colapsó, ni se produjo una revuelta popular. No obstante, fue una victoria para el Norte. "El ataque sorpresa causó un fuerte impacto en la opinión pública de Estados Unidos, que comenzó a rechazar la guerra y a retirarle su

[6] Quiao Liangand Wang Xiangsui, Unrestricted Warfare – China´s Master Plan to destroy America, Ed Pan American Publishing Company, Panama City, Panama, Año 2002, P.37

apoyo", señaló un periodista de la BBC [7]. Quien fuera Comandante de la Coalición en la Guerra del Golfo I, general **Schwarzkopf** , había participado en la Guerra de Vietnam con el grado de Mayor, y al mismo tiempo, su hermana Ruth manifestaba en Washington DC en contra de la guerra. Fue por eso que la preocupación del general por la influencia de los medios fue grande, tanto en la invasión a Granada de 1983 donde fue 2do Comandante, como en la Guerra del Golfo I [8].

Con los adelantos tecnológicos en información y comunicaciones, esto era posible, puesto que nada aseguraba si la información que se difundía para formar opinión era verdadera, falsa o tendenciosa. Surgió así la palabra *desinformación*, significando ideas falsas. En idioma ingles se hace una distinción; una cosa es *desinformation* que significa mentir con toda intención, y la otra *misinformation* que significa errores involuntarios en la difusión de información. Lo que tienen en común es que influyen en la opinión de la gente, que afecta el ejercicio del poder de quienes lo detenten.

Cuando el hombre llegó a la Luna en 1969, se trasmitió por televisión. Un amigo me comentó que lo estaba mirando con su abuelo, y el hombre le dijo; "es increíble con la edad que tienes, que creas esas cosas". ¿Habremos llegado a la luna, o fuimos informados que llegamos a la luna?

Pero nada es comparable a los efectos de la tecnología en la creación de realidades, y en este aspecto, lo que nos domina son los teléfonos móviles. No solo invaden nuestras vidas, sino que nos hace parte de estadísticas de comportamientos predecibles en las redes sociales. Esto daría para mucho hablar, pero no es el propósito de este libro.

La tecnología nos ha permitido automatizar una serie de artefactos que antes eran desempeñados por hombres, y ahora es automático. Estaríamos asombrados de saber todo lo que se maneja automáticamente, desde el transporte aéreo, hasta la apertura y cerrado de esclusas, las luces del tráfico, las plantas de electricidad y la

[7] Last Alex, ¿Qué fue la ofensiva del Tet y por qué terminó por sacar al ejército de EE.UU. de la guerra de Vietnam?, artículo de BBC News del 3 de Febrero de 2018, disponible en https://www.bbc.com/mundo/noticias-internacional-42925604

[8] Schwarzkopf Herbert Norman, Autobiografía, nombre en inglés It doesn´t take a heroe, Plaza y Janes Editores, Globus Communications, Madrid, Ed 1994, Ps. 370, 409, 423, 452, 459, 468 y 500

distribución de encomiendas. En cierta manera, el hombre se ha hecho dependiente de la tecnología. En la esfera militar, lo principal que se ha automatizado es los sistemas de comando y control, aunque también lo han hecho los sistemas logísticos, los fuegos, las maniobras y movimientos, la seguridad de las tropas y la toma de decisiones a través de la información que puede ser errónea, o falsificada.

Estos sistemas pueden ser atacados, y los efectos pueden ser devastadores, aún peores de lo significaría un enfrentamiento de fuerzas armadas convencionales. Hay otra manera de derrotar a un adversario sin emplear la fuerza militar: la opinión pública manipulada. Aquí hay dos posiciones encontradas, y es sobre el ámbito de la información.

La información en operaciones de guerra militares y no militares

Una postura es la que sostiene Estados Unidos y a la que adhiere Occidente: las operaciones de información y en ellas están incluidas el manejo de las redes sociales, se llevan a cabo en época de conflicto armado, o en instantes inmediatamente anteriores a que se desate un conflicto armado. En esta postura, para que haya un conflicto armado deben necesariamente enfrentarse medios militares convencionales y no convencionales. De esa manera, todas las operaciones de información para interrumpir, distorsionar, deformar o hacer equivocar al proceso de toma de decisiones del adversario, son operaciones complementarias a las operaciones militares. En el nivel operacional de guerra, se reflejan en líneas de operaciones lógicas, para apoyar la obtención de los puntos decisivos. Los críticos de esta postura arguyen que se debe al predominio de una mente militar estrecha, que no concibe un conflicto violento o guerra, sin que existan dos fuerzas convencionales enfrentadas, cuando las guerras del S XXI son *sin restricciones*.

La postura de occidente puede resumirse en lo que expresa el artículo **The Insufficiency of U.S. Irregular Warfare Doctrine**, cuando sostiene que:

> *Si bien están alertas de estas amenazas, los estrategas de EEUU luchan por definirlos, como queda evidenciado por el uso frecuente de términos mal definidos y no doctrinarios como como híbrido, zona gris, no tradicional, guerra sin restricciones y asimétrica. Los términos doctrinarios guerra*

> *irregular (IW) y guerra no convencional (UW) proporcionar un punto de partida común para la discusión, pero están incompletos, generalmente no se entiende bien, y a menudo mal utilizados* [9].

Significa que para la doctrina estadounidense, lo único definido es la guerra irregular o guerra no convencional. Los otros términos no son doctrinarios y por lo tanto, las Operaciones de Información son un complemento de las operaciones militares convencionales y no convencionales. No obstante, hay que estar alerta que esa no es la única concepción.

Para Rusia y China, las operaciones de información sirven para la obtención de objetivos estratégicos, y se emplean en todos los campos del poder nacional y no solo en el campo militar. Aunque no aceptan totalmente el concepto de escenario híbrido y prefieren denominarlo *escenarios no lineales*, aceptan que las operaciones para obtener los objetivos estratégicos pueden ser operaciones convencionales, no convencionales y de cualquier otro tipo incluso las caracterizadas como delictivas. En el pensamiento ruso, Occidente está permanentemente atacando a Rusia en cada uno de estos campos y los medios militares convencionales deben reservarse para las últimas etapas y solo si son estrictamente necesarios. Para los chinos, todo se resume en su primer principio de la guerra: "Usted pelee con sus medios y modos, que nosotros pelearemos con los nuestros".

El que ha descripto esta concepción rusa es el General **Valery Gerasimov**, aunque hay muchos otros pensadores rusos que opinan lo mismo.

> *"Ha surgido un nuevo tipo de guerra, en la que la guerra armada ha abandonado su lugar decisivo en el logro de los objetivos militares y políticos de guerra a otro tipo de guerra: guerra de información"* [10].

---

[9] Pellerity y otros, The Insufficiency of U.S. Irregular Warfare Doctrine, artículo publicado en Joint Forces Quarterly JFQ 93, Segundo Cuatrimestre 2019, P. 104

[10] V. Kvachkov, Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html (accessed 21 July 2016). Citado por Giles Keir, Handbook of Russian Information Warfare, monografía del NATO Defense College, Noviembre 2016.

Alguien se dio cuenta que con la proliferación de TIC la opinión pública, base de la democracia, podía ser fácilmente manipulada. La opinión pública no era el pensamiento reflexivo de la gente, porque en general no se educa para pensar con pensamiento crítico acerca de lo que es mejor o lo que es peor. La gente se impresiona más a través de los sentidos, por razones viscerales, por la voz, por la presencia de quien hable, por los que se denomina "asesores de imagen". Lo otro es que el poder económico domina los medios de información, las ideas se pueden inculcar para que juzguen especialmente por lo que ven en televisión, y no piensa en lo que se le puede ocultar. Entonces más que opinión pública, correspondería decir la opinión mediática.

La dimensión social de la manipulación y la desinformación se examina en términos de abuso de poder por los que tienen acceso preferencial al discurso público y manipulan el pensar colectivo a favor de sus propios intereses. Desde que se inventó la edición de videos, falsificar una noticia es extremadamente sencillo. En esta imperdible breve charla, el reconocido sociólogo y filósofo estadounidense **John Millburgh**, se pregunta de un modo contundente y poco convencional cuáles son los fundamentos de nuestras creencias, y concluye que la realidad nuestra está construida por la información [11].

Igualmente aleccionador son los videos de Argentina Visión 2020/2040 **7mo Encuentro de Reflexión**, del 13 de Junio de 2019 l Centro Cultural de Ciencias [12], donde habla **Santiago Bilinkis** acerca de la manipulación de datos en las redes sociales, y el video de J**ennifer Golbeck** sobre la forma en que se usan y manipulan las redes sociales donde demuestra como los "like" de Facebook inspiran sobre los rasgos de la personalidad de quien lo hace [13].

En virtud que los que lean estas líneas serán expertos en el asunto de datos manipulados en las redes sociales, es de imaginar que cada vez

[11] Millburgh John,Teed Bariloche, Por qué creemos en lo que creemos, Septiembre de 2019, disponible en https://www.ted.com/talks/john_millburgh_por_que_creemos_en_lo_que_creemos?language=es

[12] Bilinkins Santiago, Argentina Visión 2020/2040, 7mo Encuentro de Reflexión, del 13 de Junio de 2019 l Centro Cultural de Ciencias, disponible en https://www.ted.com/talks/santiago_bilinkis_como_nos_manipulan_en_las_redes_sociales?language=es

[13] Golbeck Jennifer, video "Your Social Media "Likes" exposes more than you think", abril de 2014, disponible en https://www.ted.com/talks/jennifer_golbeck_your_social_media_likes_expose_more_than_you_think

que bajan una aplicación, leen con todo detalle las condiciones en letra chica antes de aceptarlo, o quizás acepten sin leer nada apremiados por la urgencia. De cualquier forma, sería bueno que investigasen el caso de **Cambridge Analytica** una consultora especializada en recopilación y análisis de datos para campañas políticas y publicitarias, su sospechado rol en las elecciones abiertas de Estados Unidos en el 2016 y la denuncia de manipular y usar datos en **Facebook.**

En suma, esta abrumadora revolución en tecnologías de información y comunicaciones ya casi se ha constituido en una Revolución en Asuntos Militares. Las guerras ya no se desarrollan en la estrecha visión de ver dos ejércitos enfrentados, sino que se trata de una guerra total donde es difícil diferenciar paz y guerra, y donde los medios no militares tienen tanta o más importancia que los medios militares.

Para los rusos, y para los chinos, se trata de una nueva forma de guerra. En palabras del General **Valery Gerasimov**,

> *Las mismas "reglas de guerra" han cambiado. El papel de medios no militares de para obtener los objetivos políticos y estratégicos ha crecido, y, en muchos casos, ellos han excedido el poder de la fuerza de las armas en su efectividad* [14].

Antes de comenzar un análisis hay que comprender que lo importante es que mientras el occidente considera estas medidas no militares como una manera de evitar la guerra, Rusia considera estas medidas como guerra.

> *Rusia cree que el patrón regímenes de fuerza patrocinado por Estados Unidos ha sido suplantado en gran medida por un nuevo método. En lugar de una invasión militar abierta, los primeros intentos de un ataque estadounidense provienen de la instalación de una oposición política a través del estado mediante propaganda (por ejemplo, CNN, BBC), Internet y redes sociales y organizaciones no gubernamentales (**ONG**). Luego de instalar con éxito la disidencia política, el separatismo y / o la lucha social, el gobierno legítimo tiene dificultad creciente*

[14] Coalson Robinso, Editor, The value of sciencie in the foresight, traducido del Ruso el 27 de Febrero de 2013. Military Review January Februeary 2016, P. 13

> *para mantener el orden. Como la situación de seguridad se deteriora, los movimientos separatistas pueden ser alentados y fortalecidos, y operaciones especiales no declaradas, fuerzas militares convencionales y privadas (contratistas de defensa) pueden ser introducidas para luchar contra el gobierno y causar más estragos* [15].

Quiere decir que mientras para Estados Unidos y Occidente las operaciones de información declaradamente son un complemento de las operaciones convencionales, para Rusia son parte de una nueva forma de hacer la guerra en desarrollo donde se busca evitar el uso de los medios militares convencionales, para obtener los objetivos políticos y estratégicos.

La discrepancia es que Occidente piensa que ese modo de hacer la guerra lo hizo y hace Rusia en Estonia, Georgia, Crimea, Ucrania y Siria, Rusia piensa que Estados Unidos y la NATO lo hace intentando avanzar con sus fronteras geográficas hacia el Este.

China, por su lado, y conforme lo sostienen los Coroneles del EPL **Quiao Liang** y **Wang Xiangsui** en su obra "**Unrestricted Warfare**",

> *Aunque los límites entre los soldados y los que no son soldados se haya desvanecido, y el abismo entre la guerra y no a la guerra ha sido casi rellenado, la globalización ha hecho todos los difíciles problemas interconectados y entrelazados y nosotros debemos encontrar una clave para ello. La clave debe ser capaz de abrir todos los bloqueos, si estos bloqueos están en la puerta principal de la guerra. Y esta clave debe ser adecuada para todos los niveles y dimensiones, desde la política de guerra, la estrategia y las técnicas operacionales a las tácticas; y también debe ajustarse a las manos de los individuos, de los políticos y los generales, hasta a los soldados comunes. No podemos pensar en ninguna otra clave más apropiada que la "guerra sin restricciones"* [16].

---

[15] Bartles Charles, Getting Gerasimov Right, artículo de Military Review January February 2016, P. 32.

[16] Quiao Liangand Wang Xiangsui, Unrestricted Warfare – China´s Master Plan to destroy America, Ed Pan American Publishing Company, Panama City, Panama, Año 2002, P.191

La estrategia china se basa en principios diferentes a los convencionales para el ambiente clásico del Mariscal **Foch** a comienzos del Siglo XX. Salvando la brecha del idioma, en el Siglo XXI son llamativos dos: T*u usas tu método de lucha, yo uso método mío*, y resaltando la importancia de la opinión pública: *Una causa justa goza de abundante apoyo, una causa injusta encuentra poco apoyo*. Elaboran diciendo que adherirse a los principios de la guerra justa, puede movilizar a la mayor cantidad de personas, y así se ejerce el poder general de la guerra popular.

En Occidente, las libertades individuales, el derecho a expresar libremente las ideas, el derecho al disenso, el derecho a la privacidad, el derecho a un juicio justo, el derecho a no ser juzgado por leyes posteriores a los hechos que se imputan, y la defensa contra los abusos del poder y demás derechos civiles han sido pilares de las sociedades desde que los barones en 1215 obligaron al monarca inglés **Juan Sin Tierra** a aceptar la Magna Carta constituyéndose en la fundación del derecho internacional, y del derecho de la libertad del individuo contra una autoridad arbitraria y los abusos de poder.

Hoy esas libertades individuales están cada vez más coartadas por los controles sociales necesarios para vivir en orden en una población en constante aumento. Eso es contradictorio en sociedades donde la democracia, entendida como la opinión de las mayorías, se adopta por una opinión pública que en realidad se ha transformado en opinión mediática que puede ser manipulada por el poder político y económico que busca mantenerse o conquistar el poder. La información es poder, y habrá que aceptar una intromisión cada vez más frecuente en esferas que antes se reservaban exclusivamente a las libertades individuales.

De manera tal que aunque se esté inadvertidamente en un bando o en otro bando, hay que asumir que estaremos bajo constante ataque. Los países no estarán solos, y necesitarán conformar alianzas con países poderosos que serán competidores. Este sistema de alianzas es de un equilibrio inestable, porque los países periféricos recibirán una cuota de poder del país repartidor de poder que se reflejará en bienestar para sus ciudadanos. Como cada actor pugnará para obtener más beneficios, el equilibrio será inestable. Asimismo, se deberá asumir que asociarse a un país que compite con otro país repartidor de poder resultará en desventajas y actos punitorios.

Ya sea en una concepción de uso de las operaciones de información, como en la otra, hay que partir del supuesto que seremos atacados. Es algo imposible de detener. También hay que asumir que en algún momento cibernéticamente seremos invadidos por alguien que no sabemos dónde está, si es un Estado o un particular, si es un ingeniero informático o un aficionado del colegio secundario.

Habrá que hacer también consideraciones sobre la actitud defensiva. Como sostenía **Clausewitz**, la superioridad de la defensa sobre el ataque es que atrae el enemigo al terreno que elija el defensor. Además, lo encasilla en una oportunidad que le es favorable. En nuestra imaginación, el defensor es como un guerrero con escudo que soporta los mandobles de la espada del enemigo. Sin embargo, todos aceptarán que si esa es la figura, en algún momento el defensor se cansará, y el atacante triunfara. A menos que el defensor espié por el costado del escudo para avizorar el miento que el atacante se cansa, para tirar su propio golpe y así, el atacante no blandirá más su espada en contra nuestra, y estaremos más seguros. Eso se llama ofensiva.

De donde, en operaciones cibernéticas, se hará difícil distinguir ofensiva de defensiva, aunque éste no es el riesgo más grande.

Lo que sí es seguro es que todos negaran responsabilidad. Así que hay varias conclusiones sencillas 1) políticamente, hay que buscar el aliado cibernético repartidor de poder que más convenga a los propios intereses; 2) esa alianza en el espacio debe ser una política de Estado, de carácter permanente, y no voluble 3) esa alianza repartirá no solo beneficios, sino también nos hará sufrir perjuicios; 4) nos atacarán y será difícil saber quién y cuando; 5) ante esta eventualidad, hay que estar en condiciones de defendernos: 6) es casi ineludible en algún lugar el o los atacantes tendrán éxito; 7) por eso, tenemos que hacer los sistemas redundantes y resilientes; 8) para eso, tenemos que tener back up recientes de todos los archivos y sistemas; 9) hay que estar preparado para atacar, con la finalidad de defenderse; 10) puede atacar para que el atacante cese en su ataque, pero en su carácter de país periférico, asegúrese que todo lo que se haga a ese efecto pueda ser desecho por usted mismo.

El riesgo más grande es que la desinformación, la manipulación y las redes sociales venzan el espíritu de resistencia de los hombres a la

dominación, haciéndoles ver como favorables a situaciones que van en contra de sus intereses legítimos, y su bienestar.

Es el poder de la información. Por eso Occidente tiene Internet, y China su sistema propio **QQ**, Se ha acusado a QQ de ser cómplices del programa gubernamental chino de censura y espionaje, ya que permitiría que las autoridades pudieran observar las comunicaciones de sus usuarios. Rusia tiene su sistema **rusnet**, que es el intranet de Rusia. La información es un arma de dominación, de las más poderosas existentes porque ataca la mente de los hombres.

Al menos declaradamente para Rusia y China, la información se convirtió en una nueva e inadvertida naturaleza, propósito y forma de conducir la guerra del S XXI.

4. Concepto físico de Resiliencia.

Ya hemos hablado algo sobre resiliencia, ahora vamos a comenzar a profundizar en su base técnica, para seguir avanzando luego acerca de todo lo que implica en nuestras redes y sistemas.

Como muchos otros conceptos de esta nueva y reciente ciencia de la informática, sus bases se hallan en ideas y teorías presentadas por otros ámbitos sobre las cuáles se continúa creciendo y generando relaciones que aplican a las redes y TI.

En el caso de la Resiliencia, podemos pensar que la idea inicial nace de la física o también de la sicología, pues nos presentan las siguientes definiciones mucho antes del nacimiento de los ordenadores (*Conceptos tomados de https://es.wikipedia.org*):

Definición sicológica de resiliencia:

> *"Capacidad de los seres humanos para adaptarse positivamente a las situaciones adversas. Resiliencia viene del término latín resilio, «volver atrás, volver de un salto, resaltar, rebotar». El término se adaptó al uso en psicología y otras ciencias sociales para referirse a las personas que a pesar de sufrir situaciones estresantes no son afectadas psicológicamente por ellas*
>
> *Asimismo, la resiliencia es la capacidad de tener éxito de modo aceptable para la sociedad a pesar de un estrés o de una adversidad que implica normalmente un grave riesgo de resultados negativos"*.

Definición en ingeniería de resiliencia:

> *"Se llama resiliencia de un material a la energía de deformación (por unidad de volumen) que puede ser recuperada de un cuerpo deformado cuando cesa el esfuerzo que causa la deformación.*

La resiliencia es la propiedad que representa la capacidad de un material de recuperar su forma luego de sufrir una deformación".

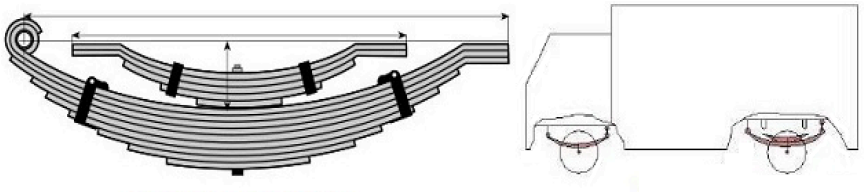
Como dato significativo y que me ha llamado la tensión en estos conceptos de Wikipedia es que: "*Entre los materiales conocidos mas resilentes se encuentra la seda de araña (**4500** kJ/m3), el tendón (2800) o el cuerno de mamíferos (1800). El acero en cables presenta un resiliencia elevada (**900** kJ/m3)"*… Es decir que una tela de araña es 5 veces más resiliente que un cable de acero… nuevamente la naturaleza tira por tierra los más importantes descubrimientos de esta raza humana que nos creemos todopoderosos…

Como podemos apreciar en ambas definiciones, este concepto se refiere a la capacidad de recuperación.

Pidiendo disculpas por anticipado a cualquier físico teórico que lea estas líneas, intentaré presentar este concepto, dejando de lado su cálculo y fórmulas, para desarrollarlo de forma sencilla.

El concepto que siempre me ha resultado sumamente representativo es el del alambre negro, ese que en Argentina se usa para reparar absolutamente todo (*y más…*), el alambre de campo. Este material esta compuesto únicamente por hierro, es probable que todos nosotros alguna vez hayamos hecho algo con alambre y sabemos perfectamente que al doblarlo tiende a mantener esa forma que le hemos dado. En física se lo denomina "comportamiento plástico" y se trata de la respuesta de un material, que al ser deformado, justamente no se recupera. El caso bastante diferente es cuando ese hierro se funde con carbono dando como resultado el acero, en general un acero debidamente templado y revenido tiene un alto "comportamiento elástico", es decir si uno lo deforma tiende a retornar a su estado inicial.

Para seguir siendo prácticos, hagamos un poco de memoria y recordemos esos coches viejos o carruajes de caballos, e inclusive hoy en día aún lo siguen usando camiones y otros vehículos industriales para evitar los sacudones del camino. Hace años se ha inventado el sistema de suspensión, por medio de elásticos, diseñados con flejes de acero en forma



Ballesta y Ballestín

de arco, de mayor a menor longitud y unidos por un suncho, este tipo de sistemas se los suele llamar de "ballesta". El chasis y carrocería del vehículo apoya sobre sus extremos y en el centro del la ballesta se sostiene el tren de ruedas (*o eje de ruedas*). Cuando la rueda pasa por un badén o pozo, se deforma la ballesta y como su comportamiento es "elástico", rápidamente recupera su estado anterior al pozo.

Lo que acabamos de presentar en este viejo sistema de vehicular es justamente un sistema que recupera su estado inicial ante deformaciones o cambios de estado.

Por supuesto que, si sobrecargamos el peso del vehículo en exceso o impactamos contra un desnivel importante, todo el sistema puede sufrir un daño irreparable o llegar a romperse. Si se rompiera, físicamente lo llamarían "Umbral de rotura", situación que cualquier diseñador o propietario del vehículo trataría de evitar.

También se debe tener en cuenta que no existe un material o sistema totalmente elástico o totalmente plástico. Es probable que alguna vez nos haya sucedido el hecho de estirar un alambre de hierro negro (cuya *naturaleza, reitero, es plástica*), por ejemplo una varilla del mismo más o menos larga, supongamos algo así como un metro de largo, si la fijamos en un extremo, y deformamos uno o dos centímetros el otro, seguramente retorne a su posición recta, es decir tendría su cierto comportamiento elástico. También es de considerar un cuchillo de cocina de acero, por ejemplo, Tramontina (*de origen Brasileño, muy bueno y uno de mis preferidos*), el cual de forma justificada para cualquier ser humano sediento, es empleado ante un estado de emergencia total al no tener abridor de botellines de cerveza, para hacer palanca en su tapa de metal, y su punta queda doblada (es decir no retorna a su estado original), pues en esta caso, luego de beber la cerveza, notaré que no ha tenido un buen comportamiento elástico.

Reflexión 1:

Límite (*umbral*) elástico, plástico o de rotura.

Si seguimos avanzando en este tipo de comportamiento físico, también merece la pena tener en cuenta, tal cual hemos mencionado, que no existe ningún material puramente plástico o elástico. En el caso de una vieja tiza (*otro elemento en extinción*), esa que los que peinamos canas, vimos que empleaban nuestras maestras en la escuela; seguramente recordamos lo sencillo que era partirla en trozos para no escribir con la tiza entera, o

también para hacer guerras con estos pedacitos en el aula… La tiza o el cristal son muy buenos ejemplos de "rigidez".

Por otro lado, manteniendo los enseres de oficina o de clase, también podemos presentar las conocidas gomitas o tiritas elásticas, esas que en el banco emplean para enlazar los billetes, cada vez que pasamos por su ventanilla previendo un próximo corralito (o de las extrañamos por no poder retirar efectivo, luego del corralito…), que también son de sumo interés en las mismas guerras escolares. Este tipo de elementos o material, se denomina flexible (o también elástico).

Es lógico pensar que ninguno de estos comportamientos extremos sería adecuado para la ballesta de ese carruaje, si queremos que el sistema retorne a su estado inicial, se debe encontrar el equilibrio justo entre estos comportamientos.

Reflexión 2:

Equilibrio entre rigidez y flexibilidad.

Este equilibrio, o relación coste beneficio, no sólo se debe a factores técnicos del material, sino también a la calidad del mismo, o mejor dicho a la calidad de TODOS los componentes de mi sistema. Con excepción de estos días, en los últimos años hemos vivido una enorme invasión de todo tipo de elementos provenientes de China o Taiwan. Ahora la calidad de los materiales de allí provenientes está mejorando mucho, pero al principio hemos visto llegar artefactos "de un solo uso" pues se rompían a los minutos de emplearlos. También hemos tenido a lo largo de la historia como referente la industria Alemana, donde es prácticamente sinónimo de garantía la calidad del material que se adquiera.

En muchas oportunidades hemos podido verificar que la "calidad" no siempre es una cuestión de precio, y la relación coste/beneficio en el empleo de un determinado material u otro, merece la pena ser considerado en detalle a la hora de diseñar cualquier tipo de despliegue o desarrollo.

La "Resiliencia" de un sistema va muy de la mano de la calidad que empleemos en el mismo.

Jamás me olvido de esas viejas neveras "Siam" pioneras en los sistemas de refrigeración de alimentos en todo el mundo. En la casa de mis padres la siguieron usando por más de cuarenta años. Siguieron saliendo marcas y modelos, la Siam no era la más cara, sin embargo era eterna.

Creo que muy pocos dispositivos en mi vida fueron más representativos de este ejemplo que mi querida nevera Siam.

Reflexión 3:
Calidad del material (*no necesariamente precio*).

Continuando con la industria automotriz, en el año 1986 compré un Citroën 3CV, lo desarmé entero y lo convertí en un Mehari (*era precioso*). El sistema de suspensión en este tipo de coches, a diferencia de los convencionales con la "ballesta" mencionada, o con el espiral más que conocido, funciona por "torsión". El tren de ruedas que es independiente en cada una de ellas, cuestión muy novedosa en su época, va sujeto a un brazo de palanca que posee una "barra de torsión" que en cada eje, une ambos extremos de los dos brazos de palanca, rueda izquierda en un extremo y rueda derecha en el otro, y lo mismo en cada tren (delantero y trasero). Cuando cualquiera de las ruedas pasa por un desnivel, ese brazo de palanca, deforma (retuerce) la barra de torsión que le permite asumir el pozo subiendo o bajando y luego retorna a su estado inicial.

Si comparamos este sistema de suspensión con el de ballesta, vemos perfectamente que este funciona por "torsión" y la ballesta por "presión". Lo mismo podríamos pensar sobre la gomita (o tirita elástica) del punto anterior, la cual funciona por "tensión". También tenemos sistemas que son Resilientes, o no, a otros factores como puede ser electricidad, temperatura, humedad, fuego, rayos UV… Es decir un sistema sistema no es resiliente "per sé", sino que debemos considerar "Resiliente a qué"

Reflexión 4:
Resiliente a qué.

Uno de los aspectos más pintorescos que tiene un Citroën es su andar como en "olas", hasta era divertido circular en el mismo, pues cada vez que pasabas un pozo subía y bajaba atenuándose poco a poco, era como si circulases en canoa luego que pasa una embarcación grande subiendo y bajando hasta que la ola se minimizaba.

Este comportamiento, si bien es pintoresco tal cual dije al principio del párrafo, a medida que pasan los años (*en todo sentido*) suele ser cansador y uno es como que va prefiriendo un sistema de suspensión un poco más moderado y que "amortigüe" mejor los baches. Nuevamente volviendo a nuestro concepto madre de equilibrio, por supuesto que alguna que otra subida y bajada deberé soportar siempre, en todo coche o, casi, casi, casi, que en todo lo que se refiere a la vida misma, lo que se trata nuevamente es buscar la justa relación en esta idea de "amortiguación" y que todo el

Reflexión 5:
Amortiguación (rebote).

diseño e implementación de este tipo de sistemas no sea un mero "rebote".

Machacando un poco más sobre esta idea de "rebote". Cuando un sistema se deforma y amortigua, independientemente que se desee el equilibrio sobre la amortiguación, también es muy importante de evaluar en que tiempo se recupera a su estado inicial.

Insistiendo sobre los casos prácticos y ejemplos simples, esta idea por mi parte siempre se me representa a través de los diferentes sistemas que se emplean para cerrar puertas automáticamente, una vez que se abren a mano. Pocas cosas en la vida me resultan tan desagradables como entrar a un sitio, abrir un puerta incautamente, pasar a lo largo de ella, soltarla y pegarme un susto al sentir el violento portazo a mi espalda motivado por un pésimo diseñador que no pensó en el grueso de la humanidad y el tiempo que emplea el sistema de cierre que oscila en los pocos nano segundos. Por el contrario me resultan sumamente gratificantes estos sistemas modernos de cierre, tanto de puertas como de cajoneras, en los cuáles da gusto abrirlos y cerrarlos, y hasta les quitamos vida útil, pues en vez de abrirlos una vez sola para obtener un tenedor, volvemos a hacerlo un par de veces más por lo placentero que es apreciar el genio de quien los pensó con ese suave sistema lento, sin ruido, aceitado y ajustado al tiempo exacto de respuesta (*me da bienestar el solo recordarlo…*).

Reflexión 6:

Tiempo de respuesta óptimo.

En resumen, jamás olvidemos la idea de "Tiempo de respuesta óptimo".

Como me gustan los coches, retorno a mi Citroën Mehari (*que era precioso*), y así como lo desarmé y lo volví a armar al completo, a su vez, también por varios factores, entre ellos tal vez el principal era que en esa época no me encontraba muy suelto de dividendos, el mantenimiento del mismo lo hacia totalmente yo, jamás pisó un taller. Claro en esa época la mecánica era entendible y accesible, hoy en día el mantenimiento que le hago a mis coches, es prácticamente nulo. También reconozco que por distintos motivos, muy diferentes a los de mi querido Mehari, pero tal vez el principal se deba a que el esfuerzo de mantenimiento responde a otro tipo de factores.

Hoy en día la mecánica de un coche es inaccesible, hace falta un ordenador para su diagnóstico, otro para su puesta a punto, un conjunto de instrumental que solo lo tienen los talleres oficiales, los cuáles a su vez ya no reparan casi nada, son meros "cambia piezas" completas (por costosas que sean las mismas).

Considerando este nuevo planteo y volviendo a nuestra razón de ser en la vida, a través del omnipresente equilibrio, también se debe tener en cuenta que la resiliencia de todo tipos de sistema (coche incluido) también debemos analizarla sobre la base de su esfuerzo de mantenimiento. A cualquiera de los lectores le tiene que haber generado dudas al cambiar de coche, si es mejor un coche que viene con garantía de mantenimiento incluida por cinco años u otro que ofrece dos, o uno usado que ya no posee ninguna.

También seguramente hemos tenido el dilema entre diferentes marcas y modelos cuyo mantenimiento se conoce que es menor o mayor, o sus recambios son más o menos económicos, o sólo ofrecen garantía en sus talleres oficiales, o son marcas que se reparan fácilmente en cualquier taller, etc.

Lo que sí afirmo categóricamente es que ningún lector de este libro ha tenido que decidir entre un Ferrari, Lamborgini o Masseratti, pues de ser así no estaría perdiendo el tiempo con esta lectura.

En resumen, para que el concepto de resiliencia pueda ser estable a lo largo del tiempo, es necesario valorar qué esfuerzo de mantenimiento requiere.

Reflexión 7:

Esfuerzo de mantenimiento.

En adición a mi afición por los coches y la mecánica, todos los que me conocen saben que "**yo voy en moto**" por la vida (*así se llama una de mis canciones y videos:* https://www.youtube.com/watch?v=MUQC8tZtFwc), llevo con ellas desde hace cuarenta y cinco años.

Esto viene a cuento, pues un verano la llevé a mi querida playa de Villa Gesell - Argentina, fue inolvidable. Hicimos paseos por todos los médanos y llegamos hasta esas playas que años atrás eran casi desiertas y hoy están saturadas, por supuesto y como buen joven en esos años, en las zonas donde el mar nos lo permitía, circulaba con la moto por la orilla salpicando agua a ambos lados, fue un verano de aventura total.

Mi sorpresa fue cuando unos meses después, a pesar de haberla lavado varias veces, los amortiguadores estaban deteriorados y comenzaron a perder líquido. Claro, cualquier persona en su sano juicio sabe que el agua de mar corroe y genera pequeñas fisuras que resienten el comportamiento de los materiales, en particular los metálicos, cuando uno es joven esto del sano juicio se mide con otros parámetros.

Tuve que cambiar los dos amortiguadores traseros, que en las motos van dentro de los espirales de suspensión, es decir me costó el sistema completo y en esos años de poca liquidez… hay que dolor.

Esta es otra de las cuestiones relacionadas a la resiliencia, las fisuras o degradaciones del material. En todo diseño de un sistema, se considera muy especialmente su tiempo de vida bajo condiciones normales de funcionamiento. Se trata de un parámetro que define su ciclo de vida, recorridas de manteniendo, obsolescencia y plan de renovación. Por supuesto, como vemos más adelante, en sistemas informáticos y de telecomunicaciones también.

Tal cual se acaba de expresar, estos cálculos ser realizan el "condiciones normales" de trabajo pero, tal cual sucedió con mi moto, cuando las condiciones cambian, pues también lo hace su ciclo de vida y todo el plan de diseño original. Cualquier anomalía o incidente, deseado o no, impacta directamente en la capacidad de recuperación del mismo. Volviendo siempre a nuestros ejemplos sencillos, si lo asociamos a un arco y flecha, aunque nunca hayamos usado uno, al menos lo hemos visto en alguna película. Al tensar un arco para poder lanzar la flecha lo más lejos posible, se están ejerciendo una fuerzas importantes. Dudo mucho que un buen arquero, si ve que en ese arco aparece una pequeña raja, fuera capaz de tensarlo o seguirlo usando, pues es plenamente consciente que se encuentra en una situación límite y, si al tensarlo, esa fisura llega a su "umbral de rotura" lo más probable es que sufra las lógicas consecuencias físicas (*el arco, y él mismo*).

Reflexión 8:

Fisuras (o degradación).

Asociando esto del arco y flecha, con nuestro inicial sistemas de suspensión denominado ballesta, cuyo funcionamiento, cualquiera puede apreciar que es similar; tanto es así que con muy poca imaginación así lo han llamado, derivándolo del arma medieval cuya nombre casualmente es "ballesta" que, o casualidad también, se derivó del arco y flecha… ¡cuántas coincidencias!

Este sistema de suspensión y casualidades, a lo largo del tiempo, su comportamiento "elástico" (*que ya sabemos que no es 100% así*) va cediendo y comienza a perder sus condiciones iniciales. En algunos casos esto es perceptible y en otros no, pero en concreto, el sistema de suspensión ya no es el de un cero kilómetro y se va deformando.

En los países desarrollados, como hemos mencionado, se tira todo el conjunto a la basura y se reemplaza por uno nuevo. En países donde la gente se busca la vida un poco más, o tiene la necesidad de hacerlo, aparecen estratagemas de recuperación del material usado, se desarma todo el sistema, se lo vuelve a poner en su posición inicial, se lo suele volver a templar, etc. y se lo instala nuevamente, logrando algunos años más de vida, que si bien no es como si fuera uno nuevo, pues nos permite seguir comprando comida y sobrevivir un tiempo más.

En muchos casos, la clave del éxito, más allá de cambiarlo o recuperarlo está en la capacidad de medir el grado de deformación que sufre el sistema. Si soy capaz de medirlo con cierta precisión puedo lograr recuperarlo antes que se rompa causando daños mayores o al menos recuperándolo para darle más tiempo de vida. En cualquiera de esos casos, lo que es evidente es que el sistema se deforma a lo largo del tiempo y debería ser importante ser capaz de reconocer o medir el grado de deformación sufrido.

Reflexión 9:
Grado de deformación.

Cuando era pequeño, mi padre y un tío mío, compraron juntos un coche cero kilómetros Ford Falcon (*todo un clásico entre los 60' y 90' en Argentina*).

Este modelo de coche fue famoso en todo Latinoamérica, aún se siguen viendo en circulación. Su principal característica era su fortaleza.

Para seguir centrándonos en esto de la suspensión, un hecho anecdótico, fue cuando nos reunimos años después y a ambas familias nos llamó la atención como se sacudía el coche de mi tío. El de mi papá seguía siendo una sede en su andar, sin embargo el otro se asemejaba a ese Citroën que acabamos de mencionar, su sistema de amortiguación estaba bastante deteriorado.

Nosotros vivíamos en la ciudad de Buenos Aires y mi tío en el campo. Si bien las calles de esta gran ciudad nunca se han caracterizado por su buen estado, en el campo, las cosas eran bastante peores y mi tío realizaba frecuentemente grandes desplazamientos por caminos de tierra o ripio, forzando el coche a "presiones persistentes" en su sistema de suspensión, por lo tanto, siendo los dos vehículos gemelos, uno de ellos había estado sometido a este tipo de esfuerzos en mucha mayor medida que el nuestro.

El tema de las "presiones persistentes" es un fenómeno muy importante a tener en cuenta en el diseño de todo sistema, en particular en aquellos cuya injerencia es evidente. Cuando pasemos a la parte informática, por supuesto

que impactará cualquier plataforma que esté más expuesta a Internet o cuyas prestaciones la obliguen a ofrecer más recursos, pero sin adelantarnos a ello, sigamos poniendo ejemplos de sistemas físicos o naturales. Un fenómeno que creo sorprendió y sigue haciéndolo a toda la humanidad, fue el del **puente de Tacoma Narrows** en Estados Unidos de Norte América. Este fue el que por el fenómeno de resonancia, comenzó como hacer ondas hasta que se destrozó, si nunca lo has visto, te aconsejo que lo busques en Google pues es impresionante. Esta resonancia, por supuesto es un fenómeno concreto de frecuencias, pero en resumidas cuentas, se trata de una muy pequeña presión que al repetirse, en este caso en la frecuencia adecuada, va impactando cada vez más en el comportamiento del sistema hasta que lo hace volar por los aires. Ejemplos hay miles, pero desde la naturaleza misma vemos en todas las rocas del planeta, por mas graníticas que sean, que una sencilla y débil gota de agua, las va moldeando a su gusto y placer. El fenómeno de "presiones persistentes" puede ser uno de los mayores dolores de cabeza, o sorpresas, que nos llevemos algún día sobre cualquier tipo de diseño.

Reflexión 10:

Presiones persistentes.

5. Introducción a redes y sistemas Resilientes.

Para mantener la lógica del libro, vamos a iniciar este capítulo relacionando lo que acabamos de ver con el punto de vista de Informática y Telecomunicaciones respecto a la "Resiliencia".

En el capítulo anterior fuimos presentando una serie de reflexiones que serán el punto de partida del que trataremos a continuación:

- Reflexión 1: Límite (umbral) elástico, plástico o de rotura.
- Reflexión 2: Equilibrio entre rigidez y flexibilidad.
- Reflexión 3: Calidad del material (no necesariamente precio).
- Reflexión 4: Resiliente a qué.
- Reflexión 5: Amortiguación (rebote).
- Reflexión 6: Tiempo de respuesta óptimo.
- Reflexión 7: Esfuerzo de mantenimiento.
- Reflexión 8: Fisuras (o degradación).
- Reflexión 9: Grado de deformación.
- Reflexión 10: Presiones persistentes.

Una infraestructura de redes y sistemas de TI no la podemos catalogar de resiliente o no resiliente. Me atrevería a afirmar que en ingeniería el término absoluto se acaba en los cálculos matemáticos y teorías, cuando llevamos el proyecto a la realidad, es preferible manejarse por valores de "tolerancia" o porcentajes de cumplimiento. Creo que lo más importante que he aprendido en mi formación de ingeniero es que:

Lo *perfecto* es enemigo de lo bueno

No pretendo decir que dejemos de buscar la perfección en todas y cada una de las cosas que hacemos, lo que sí, afirmo es que un ingeniero como mayor virtud debe tener la capacidad de encontrar los límites o umbrales de todo lo que hace. Cuánto más preciso sea en la definición de esos límites mayor será su capacidad ejecutiva. Todas las fases de un proyecto requerirán

este tipo de decisiones, y no sólo en el ámbito de ingeniería, sino más bien en la vida misma. En el ámbito empresarial, se traduce en la relación **coste/ beneficio** de estas decisiones, y ese balance óptimo hace ahorrar mucho dinero, tiempo, esfuerzos y dolores de cabeza.

Cuando pensamos en redes y sistemas informáticos, por supuesto que desde el punto de vista de ciberseguridad, no me cabe duda que lo óptimo es mantenerlo lo más aislado posible de todo tipo de accesos físicos y lógicos. Una Autoridad de certificación "root" claro que debe estar en un búnker, sin ningún tipo de conexión física a otro host y totalmente aislada del resto de las máquinas y de la sociedad en general. Salvo este ejemplo y alguna que otra excepción mas, cualquier empresa del siglo XXI tiene la imperiosa necesidad de exponer, en mayor o menor grado, sus infraestructuras.

El responsable de estas infraestructuras, día a día, deberá ir adoptando decisiones sobre el ciclo de vida de las mismas. "*Lo perfecto es enemigo de lo bueno*"… si para cada decisión se busca el estado de perfección, durará muy poco en su puesto.

La clave es encontrar este compromiso que venimos planteando, para ello lo ideal es poder determinar cuál sería el "umbral de rotura" de nuestra infraestructura. Si logramos tener una buen aproximación de hasta dónde aguantan nuestras redes y sistemas estaremos bien encaminados. El umbral de rotura en redes y sistemas de TI es el punto extremo ante el cual, no tenemos capacidad de recuperación, o la misma, requiere tanto tiempo y esfuerzo que nuestra organización no puede resistirlo (quiebra, queda fuera del mercado, pierde toda credibilidad de sus clientes, no puede recuperar su nivel o calidad de servicio, o la información almacenada y custodiada, etc.).

Cabe mencionar que cuando se analiza este umbral de rotura, es necesario realizarlo desde diferentes puntos de vista, pues una red o sistema de TI, no necesariamente es atacado de forma intencional por un intruso causando este efecto. Estas infraestructuras, pueden llegar a romperse en grado extremo por desastres o catástrofes naturales, por fallo en cualquier tipo de sistema (*ventilación, aire acondicionado, anti incendio, energía, anti partículas, backups etc.*), fallos humanos deseados, o no, por falta de mantenimiento periódico, por un cambio en la legislación, por aspectos económicos, por un error de un partner o proveedor, etc. Por esta razón, como veremos más adelante, es vital realizar el **análisis de riesgo** de forma metódica y sí, en particular, tomamos como referencia metodologías internacionalmente comprobadas, pues mejor que mejor.

El comportamiento plástico de redes y sistemas, por mi parte siempre me gusta asociarlo a un fenómeno muy presente actualmente en la **gran mayoría** de las infraestructuras de telecomunicaciones e informática y que muchos ignoran, o desean ignorar. En mi opinión, este comportamiento es muy común en el proceder de los intrusos que saben lo que están haciendo, y comprometen infraestructuras, poniendo su mayor esfuerzo en no ser descubiertos y pasar todo lo inadvertidos que les sea posible. Este tipo de ataques es muchísimo más frecuente de lo que se cree, tanto es así que me sumo una vez más a lo expresado por **John Chambers** (ex *CEO de Cisco*).

"Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas"

El comportamiento plástico, lo asocio directamente a este tipo de intrusiones, es decir nuestras infraestructuras están siendo hackeadas, se altera el comportamiento para el que fueron diseñadas y planificadas, se deforma su operación normal, pero los responsables NO se enteran, por lo que se mantienen "plásticamente comprometidas" sin capacidad de retornar a su estado de operación normal.

Como acabamos de mencionar, una actividad que es la clave para todo esto es el "**análisis de riesgo**". En el capítulo que sigue, desarrollaremos en detalle esta actividad, por ahora vamos anticipando que este es el punto de partida de cualquier organización en temas de seguridad. El análisis de riesgo, nos dará como resultado un detalle de dónde nos aprieta el zapato, cuáles son las posibles medidas a adoptar y, sobre todo, la criticidad e impacto que tienen y/o pueden ocasionarnos las decisiones que vayamos adoptando para enfrentar esos riesgos. Si el análisis de riesgo fue el resultado de un método coherente, aquí encontraremos la primera clave para jugar con ese umbral de rotura y la elasticidad que vayamos configurando a nuestras infraestructuras.

La dirección de nuestra organización, deberá optar por un curso de acción para la mitigación de los riesgos identificados (*reitero, lo veremos en detalle en el capítulo que sigue*), aquí esta la clave en ese compromiso de coste/beneficio que terminará definiendo el umbral de rotura y las primeras líneas de resiliencia de nuestras redes y sistemas.

Reflexión 2:
Equilibrio entre rigidez y flexibilidad.

Volviendo a la situación anteriormente planteada, avancemos un poco mas sobre ese equilibrio que deberíamos lograr entre la rigidez y la

flexibilidad de nuestras infraestructuras.

A cualquiera que lleve unos años metido en estos temas, le suena eso que la "seguridad es un trastorno para todos los operadores y usuarios" de un sistema informático. La verdad es que quien lo diga tiene toda la razón, el tema está en que la "rigidez" de medidas no haga que este trastorno se transforme en una causa frecuente de fallos y anomalías en los sistemas. Los ejemplos nuevamente son cientos, pero los más frecuentes suelen ser cuando de puro exagerados se ponen restricciones o medidas tan rígidas que NO tienen sentido, cambios de contraseñas excesivos, bloqueos de sistemas ante intentos fallidos, tiempos de desbloqueo exagerados, envíos de Log masivos que no sirven para nada, acceso a sistemas y plataformas con excesiva cantidad de saltos, reportes kilométricos que no aportan, ni esclarecen nada de nada, comités innecesarios… podría seguir varias páginas más. Cualquier responsable de seguridad que reciba más quejas que felicitaciones sobre este tipo de medidas, es porque se le está yendo la mano en la "rigidez" de su infraestructura de ciberseguridad, y si lo hace, comienzan más problemas que soluciones: su personal comienza a incumplir medidas, no presta atención al bosque de Logs que acumula, no genera reportes eficientes, evade políticas de contraseñas, allana vías de acceso, abre puertas traseras, etc. Todo ello conlleva perder el norte en la estrategia de ciberseguridad planteada inicialmente y en definitiva debilita más de lo que refuerza.

Por otro lado un sistema o red excesivamente flexible, implica que acepta demasiada presión, o llega a deformaciones excesivas. En resumen es demasiado "permisivo" en todos sus aspectos. El mayor e irrefutable ejemplo que tenemos ante nuestro ojos, no es ni más, ni menos que Internet. Se trata de la red más flexible que ha diseñado la humanidad, posee redundancias, alternativas y rutas para resistir todo tipo de anomalías, creo que debe ser la infraestructura más importante diseñada en la historia de la humanidad. Como cabe esperar, gracias a esta infinita virtud, se nos ha transformado en la mayor fuente de incidentes y dolores de cabeza de cualquier informático o teleco.

No quiero ser muy insidioso en mis conceptos, pero todos sabemos lo robusto que es cualquier sistema operativo derivado de la familia UNIX, sin embargo hay algunos otros, o tal vez "algún otro" (que por supuesto no voy a dar nombres), cuyo principal factor de diseño histórico es que sea amigable, sencillo de usar y que permite mucha flexibilidad para conectarse a lo que sea, para instalar lo que venga o para que cualquiera (sepa o no de sistemas) lo

pueda usar, es decir: sumamente flexible. En relación a lo comentado, es muy fácil encontrar estadísticas o informes de los porcentajes de vulnerabilidades de cada uno de ellos.

La relación entre rigidez y flexibilidad en las medidas de seguridad es muy difícil, en muchos casos me vendrán impuestas, pues tendré que compartir información, abrir puertos, permitir accesos, ofrecer servicios, instalar aplicaciones que no cumplen con todo lo deseado, respetar decisiones económicas o de marketing, etc. Otras veces deberé decidirlas yo mismo en virtud de los recursos que tenga asignados o, las interrelaciones entre las infraestructuras que tenga, por la capacitación o los perfiles del personal que me asignen, o también por la calidad del material que emplee como veremos en las próximas líneas.

Reflexión 3:

Calidad del material (*no necesariamente precio*).

Todos desearíamos tener un Ferrari, o al menos un Mercedes Benz… algunos llegan económicamente a comprarlo y otro no, también hay quienes tal vez tengan el dinero para adquirirlos, pero en su balance general prefieren invertir de forma más proporcionada sus ingresos y conformarse con otras marcas, en virtud del conjunto de su patrimonio. La calidad de los materiales de estos coches es indiscutible, pero de nada me sirve tener un Ferrari, si luego no puedo pagar el seguro o los cientos de litros de combustible que consume, o no tengo dónde vivir. En nuestras redes y sistemas sucede exactamente lo mismo, pero tenemos grandes ventajas a nuestro favor.

La relación coste /beneficio o calidad/precio en redes y TI, no está tan, tan, tan así como en la industria en general. En mi opinión, y lo he visto ya en muchísimas oportunidades, en nuestro terreno, la creatividad sumada y la investigación y el estudio nos ofrece herramientas potentísimas, por esta razón e que no me canso de invitar a los que me escuchan a que jamás dejen de lado el estudio y actualizaciones si se desean dedicar de lleno a ciberseguridad. Una de las más grandes maravillas que tenemos en este rubro se llama "**Open source**", y la misma nos demuestra sobre todo y sin lugar a dudas que:

Si COMPARTO —> ¡GANO!

Esta actitud de compartir conocimientos, os aseguro que nos permite vivir de ello si somos buenos en lo que hacemos, también podemos guardárnoslo e intentar vender nuestros desarrollos, programas o ideas sin que nadie acceda a sus fuentes, cosa que es perfectamente válido, pero tarde

o temprano puede suceder que salgan a la luz o se vea que son tan cerradas que el mercado tal vez deje de considerarlas rentables o confiables. Mi propuesta es poner nuestros conocimientos y capacidades al servicio del mundo informático, ver cómo crece y da frutos, y sin ninguna duda, cuando en el ambiente se vea que eso es bueno, tendré cientos de puertas que se abren. Lo afirmo de forma categórica y en gran parte por mi propia experiencia personal.

Todo este rollo, viene a cuento de que hoy en día, tenemos en el mercado productos cuya calidad es al menos igual, y muchas veces superior a las que pueden vendernos. Por favor nunca olvidéis que:

En informática y redes: "*la calidad no siempre es cuestión de precios*"

Como ejemplo, podemos hablar desde sistemas operativos completos de la familia Linux, hasta proxies, firewalls, IDSs e IPSs, servidores webs, de correo, de bases de datos, sistemas de contenidos, de vigilancia y supervisión, de video conferencia… me atrevería a afirmar que sobre cualquier tipo de desarrollo de software puede ser encontrada alguna versión Open Source del mismo.

Para implantar este tipo de desarrollos en una organización, muchas veces hay que pelearlo con uñas y dientes, sobre todo en las grandes empresas y con la alta dirección que está acostumbrada a pagar por servicios, soporte y mantenimiento, y en esta época que suele estar muy de modo el hecho de tercerizar o subcontratar estas actividades. A la hora de presentar un proyecto Open Source, se debe estar muy en claro de cómo rebatir estos argumentos, por supuesto el mejor punto de partida de nuestro discurso, es siempre el precio, pero hay que tener mucho cuidado con esta postura, pues sino sabemos justificarlo debidamente con su despliegue, soporte y mantenimiento, será difícil de convencer. Por esta razón es que una vez más caemos a las líneas iniciales: hay que estudiar y actualizarse bien.

Reflexión 4:
Resiliente a qué.

Cuando desarrollemos el detalle sobre análisis de riesgo, iremos viendo hay aspectos globales que se deben considerar, pero también que cada infraestructura tiene sus características particulares que la caracterizan. Una infraestructura no es que sea "Resiliente" o no.

Como hemos desarrollado en los conceptos físicos de resiliencia, es diferente la recuperación de un material ante un fenómeno eléctrico que de presión física, o humedad o calor, etc. En nuestras redes y sistemas de TI, sucede algo muy similar.

Partamos de un ejemplo evidente, Google debe volcar la mayor parte de su esfuerzo a ser resiliente ante incidentes con su información almacenada, en cambio una prestadora de Telecomunicaciones debe hacerlo sobre sus redes. No cabe la menor duda que la estrategia de cada una de ellas será totalmente distinta.

En un sitio clave de Sudamérica, se encuentra la instalación o parque satelital más grande del mundo (*aunque parezca une error tipográfico, sí quise decir Sudamérica y NO Norteamérica*). En estas instalaciones aún está la antena satelital desde donde se transmitió en directo a todas las televisiones la llegada del hombre a la luna, además de esta reliquia debe haber más de quinientas grandes antenas satelitales prestando servicios hoy en día. A finales del siglo pasado, con los problemas de guerrilla que azotaban varios países de ese continente, estas instalaciones guardaban un interés estratégico y para evitar cualquier tipo de sabotaje, hasta tenían un doble muro perimetral y entre ambos se encontraba todo sembrado de minas anti personal. Sí, así de serio: ¡un campo minado!, por supuesto que hoy lo han levantado, perdurando únicamente el doble muro las cámaras de vigilancia, y además: un halcón, que es el encargado de mantener las palomas bien lejos cada ve que lo sacan y lo posan en el centro del parque satelital (*ahí van nuestros grandes avances tecnológicos!!!*). Cómo podrán apreciar, uno de los mayores factores para la resiliencia que se habían planteado hace treinta años en esas instalaciones, era la seguridad física.

Deseo remarcar este tipo de "riesgos", pues fijaros la enorme diferencia; hace muy pocas semanas, estuve visitando una estación de amarre del cable submarino más veloz del mundo, mueve 160 terabit por segundo y une América con Europa. Pues uno de sus extremos se encuentra en Estados Unidos, esta vez sí de Norteamérica. El nivel de seguridad allí, y en particular en la zona donde se encuentra, que ni siquiera tiene vallado perimetral, allí el nivel de vandalismo es inimaginable que alguien se meta en una propiedad que no es suya (*muy a pesar de lo que muestran las películas*), por lo tanto, allí para mantener la resiliencia, no considera tan extrema la ocurrencia de un acto vandálico de este tipo, y hasta las autoridades locales en su momento NO permitieron el vallado perimetral.

Otro ejemplo que he vivido, fue cuando estaba a cargo de Redes del Ejército Argentino, allá por los 90'. A finales de esa década, pusimos una antena VSAT en la Antártida (*fue y sigue siendo uno de mis mayores orgullos*), tuvimos la primera conversación telefónica y acceso a datos de la historia entre ese continente y América (*y esto sucedió en Argentina…*), al poco tiempo, coincidiendo con la llegada del invierno, comenzamos a tener problemas de comunicación, luego de varios dolores de cabeza, descubrimos que el equipamiento electrónico, se encontraba en uno de los hangares de la base militar. Si el lector ha pasado frío alguna vez en su vida, puede imaginarse lo que son -40ºC, pues claro, a esa temperatura, nuestro equipamiento no se sentía muy a gusto. Tuvimos que desplazar toda la electrónica a los locales donde vivía el personal pues solo allí podíamos garantizar una temperatura superior a los cero grados. En esa base, nuestras ideas de resiliencia pasaban por la temperatura y el abastecimiento eléctrico.

Ejemplos de este tipo y sin ser tan extremos, tenemos en caudales también, desde considerar el empleo y capacidad de memoria RAM, hasta espacio en disco, alta disponibilidad, ubicaciones físicos, ancho de banda, fenómenos naturales, altura, desarrollos de software, on premises o Cloud, local y remoto, etc…

En resumen, estas particularidades de cada una de nuestras infraestructuras y/o desarrollos, necesitan se evaluadas en detalle para poder determinar, con la máxima precisión, cuáles son los parámetros fundamentales que debo prestar especial atención y reforzar que la podrán hacer resiliente o no.

Reflexión 5:

Amortiguación. (rebote).

Hace poco tiempo, me tocó lidiar con un caso muy particular y anecdótico. Un día de semana a las 12:00 hs. del mediodía se cayó por completo la infraestructura de una gran operadora de telefonía móvil, la caída duró catorce horas… Vale la pena comentar que el chiste costó más de treinta millones de dólares. El hecho fue que uno de los grandes elementos de red que emplean este tipo de redes, llevaba más de una semana generando alarmas sobre un fallo en su base de datos, dicho sea de paso, esas alarmas no las estaba mirando nadie… *ya pinta mal la cosa*… Justamente a las 12 horas, un empleado de la empresa que gestiona estos dispositivos (*un proveedor tremendamente conocido a nivel mundial*) desde su sede central, se conectó por acceso remoto para realizar tareas de rutina, y sin respetar ningún tipo de protocolos de gestión de

cambios (ventanas, permisos, privilegios, rollback y alerta al NOC…), al descubrir este fallo en la base de datos, pues ya que estaba se puso a arreglarla. Se trataba de un nodo clave en esta red, el cual por supuesto se encontraba en alta disponibilidad en configuración activo-activo, sólo uno de los nodos tenía su base de datos corrupta, el otro NO. Este iluminado y Mao dormido empleado, en vez de recuperar la base de datos buena hacia la corrupta, pues en un lapsus de creatividad, lo hizo exactamente al revés: recupero la base de datos corrupta sobre la que estaba buena… Esos nodos en alta capacidad, son los que validan y autentican las tarjetas SIM de los teléfonos móviles y a su vez tienen cargados los perfiles de los millones de usuarios dados de alta. En esta Operadora de telefonía móvil, había ocho parejas de estos dispositivos, como el diablo nunca opera solo, sino generalmente acompañado, había también un parámetro configurado con umbrales de tiempo muy ajustados, lo que ocasionó que al caerse esta primer pareja de nodos, se encolaran sus peticiones en la segunda, que por este parámetro mal configurado, solo aguantó unos pocos segundos y se cayó también. Al mejor estilo dominó sucedió lo mismo con la tercera, cuarta… y el resto de la red.

Hasta ahora solamente he explicado el desastre de la caída, pero ahora viene lo mejor de lo mejor. Cuando la operadora se desayuna del desastre, a los pocos minutos se pone en contacto con el proveedor (*mundialmente conocido*). Este gran proveedor, del cual me tocó analizar a posteriori todos los Logs para hacer la auditoría forense, puso en marcha todo su aparato de soporte de tercer nivel, pero digamos que de una forma medio pintoresca: las once personas que se pusieron de inmediato a trabajar en el incidente, lo hicieron por su cuenta y con muy escasa coordinación entre ellos… casi, casi que nula su coordinación… digamos. Pues cuando uno re configuraba "A", el otro re configuraba "B", si el tercero consideraba que había que ajustar el parámetro "C", el cuarto empleado apreciaba que era mejor reducir "D", el quinto por su parte estaba seguro que el fallo estaba en "E", pero luego que lo corregía, el sexto lo ponía de acuerdo con el parámetro "F"… y así, y así, y así, la red se levantaba, caía, recuperaba, volvía a fallar, activaba el servicio, y se encolaba en otro nodo. Nunca a lo largo de mis sesenta años de vida he vivido un caso semejante.

Un caso muy típico también es el llamado "flappeo" de las interfaces físicas de un switch. Cuando hay fallos físicos en una red Ethernet, o también cuando no se ha configurado bien la familia de protocolos de "árbol" a nivel de

enlace (STP, RSTP, PVST, MSTP o SPB), o en su caso extremo cuando se sufren ataques a nivel MAC o "Port stealing", los switchs comienzan a poner "Down" sus interfaces físicas, cuando reciben una nueva tabla de rutas, las ponen nuevamente en "Up", a los pocos segundos, al recibir una dirección MAC duplicada nuevamente, otra vez ponen esos puertos en "Down", y así entran en este tipo de bucles de comportamiento que se denomina "flappeo" y suelen se bastante difíciles de aislar y desterrar. En esos casos desde nuestros centros de supervisión y monitorización comenzamos a ver como los segmentos de la red, o en su peor expresión, redes completas, comienzan a caerse y levantarse en cuestión de segundos y de forma totalmente impredecible y anómalo.

Tanto en el primer ejemplo, como en este último, lo que podemos hacer es entrar en este juego de locuras y proceder también a lo loco. Eso sólo ocasionará que nuestras infraestructura oscile de un lado a otro al mejor estilo de una puerta "va y ven".

El concepto de "amortiguador" va directamente relacionado a la capacidad de enfocar el tema con prudencia, paciencia, de forma metódica y coordinada. Nuestra infraestructura, será mucho más resiliente, si nos tomamos el tiempo necesario para evaluar el problema, analizar sus soluciones posibles, adoptar un curso de acción eficaz y operar de forma certera, aunque parezca que podamos perder más tiempo. Lo más importante a considerar sobre los párrafos anteriormente presentados es "quedarnos con lo aprendido" para que esto no vuelva a suceder, o nuevamente: estudiar y actualizarse sobre el tema, para aprovechar la experiencia ajena y prever estas medidas. Sobre este punto de vista, es muy importante también prever situaciones y ponerlas a prueba por medio de ejercicios, simulaciones o juegos de guerra que nos permitan medir la resiliencia de nuestras infraestructuras de forma preventiva y proactiva.

Cuando comenzó el uso de las tarjetas de débito y crédito, a principio de los años 80', me quedó muy grabada la experiencia de mi abuela el día que la acompañé a su primer cajero automático para retirar parte de su pensión. Ella no podía creer que en pocos minutos pudiera disponer del importe que deseara. Su rutina jubilatoria, mes a mes, la acompañaba un par de horas en la cola del banco para que la atendiese un cajero, que sin mayo prisa rellenara los formularios pertinentes, y al cabo de varios minutos le diera en mano y en efectivo su pensión, generalmente en su totalidad, para no volver perder otra vez varias horas de su vida. Para ella, pararse frente a la

máquina, sin hacer cola y luego de apretar un par de botones, recibir mágicamente la suma deseada, rayaba al borde de lo milagroso, por su tiempo era un tiempo de respuesta maravillosamente optimizado.

Si solo esta fuera la anécdota allí hubiese quedado, pero dio la casualidad que exactamente una semana después, venía circulando yo con mi coche y también necesitaba efectivo, encontré un cajero automático, que por esos años no había tantos como hoy, pero no había donde estacionar; di un par de vueltas manzana para ver si encontraba algo sitio, y al no haberlo, aparqué en doble fila y con toda la prisa que pude, ingresé a la pequeña salita donde estaba el cajero, introduje mi tarjeta, me pidió el PIN, se tomó sus segundos, y en ese momento, otro automóvil que quería circular, me tocó bocina, para pero de mis desgracias detrás de ese coche veo un patrulla de la policía, mi tarjeta ya estaba dentro del cajero y el dinero aún no salía, y no salía y… no salía, no podía cancelar la operación, ni irme del lugar, ni hacer absolutamente nada más que mirar como el agente de policía descendía de su patrulla con toda la intención de cumplir con su deber y hacerme la bien ganada infracción de tránsito… y el dinero seguía sin salir. A veces estos cajeros, hasta parecen humanos y se contagian de los malos hábitos que tenemos las personas, creo que solo le faltaba esbozar una sonrisa sarcástica para demostrarme que no hay que estacionar en doble fila. Por supuesto esos instantes no fueron para mí un tiempo de respuesta óptimo.

En las redes y sistemas de TI, sucede algo similar, no podemos pensar que el tiempo es óptimo porque el programa que he desarrollado y la pila de protocolos que implanté responden bien. De hecho, por ejemplo en la gestión de copias de respaldo y recuperación hay un parámetro importantísimo que se denomina **RTO** (Recovery Time Objective) que debe formar parte de un buen plan de recuperación de desastres (RDP: Recovery Disaster Plan), el cual por cada sistema debe ser estudiado en particular, pues no es el mismo para cada dispositivo o aplicación, y tampoco lo es en determinadas franjas horarias o períodos pico de trabajo.

Reflexión 6:
Tiempo de respuesta. óptimo.

Ante cualquier tipo de anomalía o incidente, se debe tener muy bien definido cuál es el tiempo de respuesta óptimo y de forma detallada, con la máxima precisión y granularidad posible.

El error de ciberseguridad mas frecuente que vengo viendo es la falta de mantenimiento.

En los últimos años, la consciencia en seguridad de los administradores ha crecido y en general podríamos decir que es una preocupación cotidiana en casi todas las organizaciones. Muchas veces, se producen acontecimientos que llevan a los responsables de estas infraestructuras a mejorar el nivel que tenían. Este tipo de acontecimientos, a veces es voluntario, forzado, ordenado por alguien, en virtud de la adquisición de un nuevo elemento de seguridad, debido a alguna certificación o evento que lo impone, etc. Por alguna de estas causas, se generan acciones o medidas que logran incrementar su nivel de ciberdefensa, llegando a un umbral superior al anterior. Toda nueva medidas, acción o plataforma de seguridad que incorporemos a la infraestructura, conlleva sí o si un esfuerzo adicional de mantenimiento. Puede ser que este nivel se mantenga o mejore, pero dese mi punto de vista, existe muchas veces el error de dejar un poco de lado justamente este mantenimiento, con lo cual envejece y pierde las características normales para lo que fue diseñado.

Reflexión 7:
Esfuerzo de mantenimiento.

Siempre yendo a los ejemplos, el más clásico sucede con los IDSs e IPSs, en los cuáles si no se actualizan sus reglas y se personalizan cada una de ellas con cierta periodicidad, cada día comenzarán a aparecernos más falsos positivos y negativos hasta que el sistema termine siendo dejado de lado. Lo mismo, con la gestión de parches, antivirus, firewalls, Logs, etc.

La facilidad de automatización y virtualización que hoy en día tenemos, en muchos casos nos pueden simplificar la vida en varios aspectos, incluyendo el de mantenimiento… siempre y cuando diseñemos y planificamos rigurosamente su aplicación.

Siguiendo en la línea de la reflexión anterior, un sistema que no se mantiene actualizado, va sufriendo verdaderas "fisuras" o degradaciones en su seguridad, hasta que llega un momento en el que es muy fácil de comprometer.

Reflexión 8:
Fisuras (o degradación).

El ejemplo más típico de ello es la robustez de los algoritmos criptográficos, hace años atrás cualquier longitud de claves de mas de seis dígitos era irrompible o un algoritmo DES, o un has MD5. Cualquiera de estas funciones matemáticas en los años 90', necesitaba una fuerza computacional prácticamente inexistente en esa época, hoy cualquiera de los mencionados queda fuera de cualquier manual o guía de bastionado.

Reflexión 9:
Grado de deformación.

Otro hecho que también es importante mencionar, es que no se trata únicamente del tema de mantenimiento, otro factor a tener muy en cuenta son las estrategias de detección, tanto de ficheros, como de software o red. Es necesario planificar hitos de control de estado y estrategias de monitorización de comportamientos anómalos en nuestras infraestructuras de forma tal eu si se produce una brecha en la seguridad podamos detectarla lo antes posible para gestionarla de forma adecuada, evitando que escale privilegios y comprometa cada vez más a nuestra organización. Cualquier tipo de fisura, si es tratada a tiempo costará mucho menos esfuerzo material y humano que a medida que vaya escalando.

Cada vez que se detecta una actividad anómala en nuestras redes y sistemas, o se produce un incidente de ciberseguridad, se debe realizar un análisis forense de forma tal que se llegue determinar el grado de deformación que ha sufrido nuestra infraestructura. Esta actividad, tiene tres pilares fundamentales:

- Integridad de redes y sistemas.
- Gestión de Logs.
- Sincronización de tiempos.

Veremos el detalle de cada uno de ellos a lo largo del libro, pero como conceptos iniciales, podríamos decir, que es sumamente complicado determinar el grado de deformación de un elemento cualquiera (sea informático, físico o de lo que se trate) si no tenemos una "foto" de su estado inicial y su evolutivo hasta el instante más previo más cercano a cualquier deformación. Si no sé como se encontraba ante, será muy difícil saber cuánto ha cambiado.

En cuanto a gestión de Logs, veremos que se trata de uno de los procesos más importantes, y en particular, ante un análisis forense, pues nos permitirá seguir el rastro de toda actividad, pudiendo distinguir lo normal y cotidiano de lo anómalo.

Por último, está este aspecto muy dejado de lado, que se transforma en vital a la hora de intentar realizar una secuencia de tiempo o bitácora de actividades. Cuando el hecho afecta a más de una plataforma, servidor o dispositivo en general, si los mismos no mantienen una base de tiempo común, se hace imposible seguir la huella de una actividad.

El ultimo tema que no podemos dejar de lado, desde el punto e vista físico lo hemos presentado como "presiones persistentes", desde el punto de vista de telecomunicaciones e informática deberíamos llamarlo: amenaza persistente avanzada (**APT**: Advanced Persistent Threat), se trata de un malware diseñado específicamente para realizar ataques informáticos. Como muchos otros de estos maliciosos desarrollos, uno de sus principales factores de éxito es pasar inadvertido y mantenerse oculto todo el tiempo que pueda. Tal cual lo indica su nombre, esta clasificación solo se puede atribuir a desarrollos cuyo avanzado nivel de diseño y diferentes vectores que emplea lo hace perdurar en el tiempo y, de forma persistente, avanzan paso a paso (o gota a gota), escalan privilegios y extraen toda la información que les pueda ser de provecho para continuar en profundidad. Se ha definido también un concepto a tener en cuenta: técnicas de evasión avanzada (**AET**: Advanced Evasion Techniques) cuyo foco principal pasa por evadir particularmente sistemas de detección o prevención de intrusiones en red, en general, se basan en la fragmentación o segmentación del payload de los protocolos superiores del modelo TCP/IP de forma tal que un firewall, IDS o IPS basado en patrones de conducta o secuencias de bits, al no ver pasar el flujo completo, no los pueda identificar. También emplean técnicas criptográficas para que estos flujos de tráfico pasen de forma cifrada los mecanismos de detección, desencriptando las secuencias una vez que arriban al host comprometido.

Reflexión 10:
Presiones persistentes.

Hasta ahora los APT más importantes que se han puesto de manifiesto, fueron generados por verdaderas organizaciones mafiosas, o para actividades de ciberespionaje, y sin querer dar nombres, también casi que podríamos afirmar que hubo ciertos gobiernos involucrados en algunos de ellos, de hecho el primero de ellos fue uno de los escándalos revelados por el caso de **Snowden**.

6. Análisis de Riesgo de Resiliencia.

6.1. Conceptos previos.

Vamos a comenzar este capítulo de forma excesivamente detallada, para que podamos ir siendo conscientes del grado de importancia que tiene esta actividad.

Si buscamos en Internet el significado, veremos que:

- riesgo: Contingencia o proximidad de un daño.
- arriesgar: Poner a riesgo.

  Exponer a una persona o cosa a un riesgo o ponerlos en peligro.

Quedémonos con dos palabras claves: "exposición" a un "daño". Como ya venimos desarrollando desde el principio, nuestras redes y sistemas se ven cada vez mas ante la obligación de ser "expuestos" en mayor o menor medida. Por lo tanto, debo conocer qué piezas de mi estructura estoy exponiendo y qué grado de exposición tendrá cada una de esas piezas. También se habla de "peligro", por lo que deberé tener en cuenta a qué peligros las estoy exponiendo, o tal vez podríamos pensar a qué "amenazas" las expongo.

Al igual que en la vida cotidiana, no voy sufrir una avalancha de nieve, en el desierto del Sahara, no me va a pisar un coche en el Himalaya, o me robarán dinero si no lo tengo; en el caso de las amenazas a las que están expuestas los recursos tele informáticos, pueden ser de diferente tipo. Estas amenazas van desde desastres naturales, a actos vandálicos, fallos intencionados, o no, de tipo informático, comunicaciones, eléctrico, industrial, medioambiental, etc.

En la jerga clásica siempre encontraremos que una empresa, lo que expone son "recursos" que pueden ser materiales (hardware y software) y humanos.

No me quiero quedar sólo con estos dos conceptos, me remito al principio del libro: *Lo crítico es la "Información"… no las Infraestructuras*. Propongo que a partir de ahora, tengamos en cuenta un recurso mas que lo considero vital, la "Información" (o el dato). Algunos pueden decir que está incluido en el software, pero por mi parte, preferiría que lo tomemos como

un concepto adicional e independiente para no volver a caer que lo crítico son las Infraestructuras (que abarcan hardware y software), por favor dadme la oportunidad de tratarlo así.

En concreto nuestros recursos son:

- Humanos.
- Materiales.
- Información (o el dato).

En las definiciones también presenta "Contingencia o proximidad", es decir algo potencial, que puede ocurrir o no. En términos técnicos esto se denomina "probabilidad".

Hasta ahora tenemos entonces:

> **Recursos** que se **exponen** ante **amenazas** que tienen una cierta **probabilidad de ocurrencia**.

Una vez que identifico todos esos recursos, debo ser consciente que así como todo ser humano interactúa con otros en su desempeño organizacional, también lo hace el hardware, software y la información entre sí. Por ejemplo: cuando a través de un servidor Web, hago una consulta a una base de datos, claramente hay una *información* almacenada en un disco duro (*hardware*), que es consultada a través de un programa o aplicación (*software*), que viaja por la red hasta la Web y nos da la respuesta. Por lo tanto, no sólo es necesario la "identificación" de todos esos recursos, sino que debo tener en cuenta sus "interacciones".

Cada uno de los recursos expuestos, ha requerido un grado de esfuerzo para llegar al estado o situación actual, tanto económico, como temporal y humano, por lo que su valor será diferente en cada caso, no debo tratar de igual forma activos que requieren diferentes esfuerzos, es lógico que sobre la base de su "valoración" deba considerar el riesgo, teniendo en cuenta también que esta valoración no tiene por qué guardar relación directa con el daño que me podría ocasionar una anomalía en su comportamiento, es decir el "impacto" que puede repercutir en mi empresa un fallo en su normal desempeño.

Ampliando nuevamente, ya tenemos:

> **Recursos (Activos)**

Inter relación entre activos

Valoración

Exposición

Impacto

Amenazas

Probabilidad de ocurrencia

En el capítulo dos, ya hemos presentado esta vieja palabra "**ACIDA**".

A: Autenticación (y si queréis también "Accesos").

C: Confidencialidad.

I: Integridad.

D: Disponibilidad.

A: Accounting (o trazabilidad).

Es lógico pensar que los activos deben ser tenidos en cuenta en relación a estos cinco aspectos. La integridad de una base de datos, la Disponibilidad de un router de acceso, la autenticación de una máquina de salto o servidor de accesos remotos, la confidencialidad de los datos financieros o de I+D, cualquiera de estos recursos sufrirá mayor o menor impacto, si se analiza desde la "dimensión" que más le aplica, por lo que cada uno de estos cinco conceptos los definiremos como "dimensión".

Una vez que ya tengamos más o menos avanzado el detalle de cada uno de los conceptos que acabamos de desarrollar, es necesario seguir adelante evaluando con máximo detalle qué tipo de vulnerabilidades o debilidades están presentes en cada uno de los activos.

Sobre todo lo expuesto, se evalúan que medidas de mitigación o salvaguardas se pueden adoptar y finalmente una muy buena práctica es preparar diferentes variantes o como militarmente se llama "cursos de acción" para que la alta dirección pueda realizar su propio balance coste/ beneficio y decidir cuál es el que mejor aplica, según su propio criterio global de la organización.

Una vez que la alta dirección **aprueba** un curso de acción, se planifican y lanzan las medidas para implantarlo. En muchos casos, suele suceder que la empresa no puede decidir la adopción del curso de acción de máxima, quedando entonces fuera del alcance un conjunto de acciones que no se

implantarán, pero ya se han identificado como riesgos. Estas últimas son las que se denominan "riesgo residual" y es sumamente conveniente que la dirección firme un documento asumiendo este riesgo, pues justamente es consciente, y fue este máximo nivel, quien decidió no mitigarlo por lo que se debe hacer responsable de cualquier acción, fallo o anomalía que impacte en el mismo.

Hemos llegado al final de esta presentación de conceptos sobre lo que trata un análisis de riesgo, y nos quedamos entonces con los siguientes conceptos:

Recursos (Activos)
- **Inter relación entre activos**
  - **Valoración**
    - **Exposición**
      - **Impacto**
        - **Amenazas**
          - **Probabilidad de ocurrencia**
            - **Dimensiones**
              - **Vulnerabilidades**
                - **Salvaguardas**
                  - **Cursos de acción**
                    - *(Decisión de la dirección)*
                    - **Riesgo residual**

Ahora que hemos presentado los conceptos de análisis de riesgo, pongamos de manifiesto el título de este capítulo: "**Análisis de Riesgo de Resiliencia**".

¿Por qué razón se ha decidido llamarlo así?

Creo que lo que mejor define este título lo hemos basado en un artículo muy interesante publicado en: http://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf, cuyo título es "**Conceptualizing and Measuring Resilience**" A Key to Disaster Loss Reduction (Escrito por **K. Tierney** y **M. Bruneau**).

Esta publicación se refiere a desastres naturales y hace un análisis que merece la pena ser leído, pero lo que deseábamos destacar es que nos

pareció muy interesante esta visión que hace de lo que en inglés define como "**4R**": robustness, redundancy, resourcefulness, and rapidity.

En español, lo traduciríamos como: robustez, redundancia, inventiva (ingenio) y rapidez.

- Robustez: la capacidad de los sistemas, elementos del sistema y otras unidades de análisis para resistir las fuerzas del desastre sin una degradación significativa o pérdida de rendimiento.
- Redundancia: la medida en que los sistemas, elementos del sistema u otras unidades son sustituibles, es decir, capaces de satisfacer los requisitos funcionales, si se produce una degradación o pérdida significativa de la funcionalidad.
- Inventiva (ingenio): la capacidad de diagnosticar y priorizar problemas e iniciar soluciones mediante la identificación y movilización de recursos materiales, monetarios, informativos, tecnológicos y humanos.
- Rapidez: la capacidad de restaurar la funcionalidad de manera oportuna, conteniendo pérdidas y evitando interrupciones.

Este artículo hace referencia también a la diferencia entre resistencia y resiliencia.

- La resistencia a los desastres enfatiza la importancia de las medidas de mitigación previas al desastre que mejoran el desempeño de estructuras, elementos de infraestructura e instituciones para reducir las pérdidas por un desastre.
- La resiliencia refleja una preocupación por mejorar la capacidad de los sistemas físicos y humanos para responder y recuperarse de eventos extremos.

Por otro lado, en los dos capítulos anteriores hemos presentado una serie de reflexiones referidas a resiliencia:

Reflexión 1: Límite (umbral) elástico, plástico o de rotura.

Reflexión 2: Equilibrio entre rigidez y flexibilidad.

Reflexión 3: Calidad del material (no necesariamente precio).

Reflexión 4: Resiliente a qué.

Reflexión 5: Amortiguación (rebote).

Reflexión 6: Tiempo de respuesta óptimo.

Reflexión 7: Esfuerzo de mantenimiento.

Reflexión 8: Fisuras (o degradación).

Reflexión 9: Grado de deformación.

Reflexión 10: Presiones persistentes.

En resumen, antes de continuar con el análisis de riesgo desde un punto metodológico, creímos necesario considerar todos estos aspectos específicos de forma adicional, antes de proponer los cursos de acción, para que se presenten alternativas "Resilientes" dentro de los mismos, considerando estas "**4Rs**" y también enfoques sobre los límites presentados, el equilibrio, la amortiguación, los tiempos de respuesta, la identificación de umbrales y detección de fisuras, la supervisión de los grados de deformación y análisis continuo de presiones persistentes.

Consideramos muy importante que la alta dirección pueda tomar sus decisiones sobre cursos de acción que finalicen este análisis de riesgo contemplando todos estos aspectos que venimos desarrollando hasta aquí.

6.2. Metodologías de análisis de Riesgo.

Como siempre me ha gustado, comenzaremos esta parte relacionado a metodologías que podemos emplear, presentando los estándares mundialmente reconocidos. Dentro de ellos, el punto de partidas son las normas ISO, en este caso las de obligada referencia son:

ISO / IEC 27005 (*tercera edición en Julio de 2018*): "Tecnología de la información - Técnicas de seguridad - Información de gestión de riesgos de seguridad".

La norma suministra las directivas para la gestión de riesgos, apoyándose fundamentalmente en los requisitos de riesgos que presenta la norma ISO 27001, la que establece claramente que este es el punto de partida de todo SGSI (Sistema de Gestión de la Seguridad de la

Información). Como todas las normas ISO actuales hace hincapié en el ciclo de vida, presentando el modelo Plan - Do - Check - Act, para la gestión de riesgos. Describe aspectos fundamentales a considerar centrados en riesgos de Seguridad de la Información que comprenden: la identificación, análisis, estimación y evaluación de los riesgos, desarrollo e implementación de un plan de tratamiento del riesgo, un plan de comunicación del mismo, la supervisión, monitorización y mejora.

ISO / IEC 31000 (*segunda edición en febrero de 2018*), "Gestión de riesgos - Principios y Directrices"

Esta norma no se refiere únicamente a la gestión de riesgos de la seguridad de la información, sino que es genérica.

En realidad, al igual que la serie ISO 27000, con la ISO 31000 se definió (o se intentó definir) también una familia de normas, pero la realidad es que en la actualidad, dentro de esta serie, sólo están vigentes la que acabamos de presentar y la **ISO/IEC 31010** (*segunda edición en junio de 2019*) gestión de riesgos - evaluación del riesgo - evaluación técnicas del riesgo.

Ninguna de las mencionadas incluye metodologías para la gestión de riesgos, es decir no nos dan pautas acerca de cómo desarrollar el análisis de riesgo, pero sí son muy detalladas en los aspectos clave a considerar y por qué deben ser considerados.

Otras guías y metodologías para gestión de riesgos que podemos considerar son:

MAGERIT: Metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros "Método", "Catalogo de elementos" y "Guía de técnicas".

Pueden descargarse los tres libros en:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

NIST SP 800-30: Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos.

Puede descargarse en: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-39 "Managing Risk from Information Systems - An Organizational Perspective" is available in draft.

Puede descargarse en: https://csrc.nist.gov/publications/detail/sp/800-39/final

OCTAVE: "Operationally Critical Threat, Asset, and Vulnerability Evaluation" is a popular risk-based strategic assessment and planning technique from CERT;

Puede descargarse en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

INCIBE: ofrece una guía muy sencilla que también podemos darle una mirada: ¡Fácil y sencillo! Análisis de riesgos en 6 pasos

Puede descargarse en: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

ENISA (European Network and Information Security Agency), está ofreciendo mucha información que deberíamos tener en cuenta, pero la que considero nos puede ser de mucha utilidad es esta guía de metodologías y herramientas: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

Puede descargarse en: https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

6.3. MAGERIT.

Por tratarse de una metodología española de amplio uso en el mundo

> Queremos remarcar, que hemos tomado como referencia esta metodología por ser de amplia aplicación en el territorio español y, a su vez, porque estamos convencidos que es completa y eficiente.
>
> Resaltamos la autoría de la misma por parte de la actual **Comisión de Estrategia TIC del Gobierno de España**.

hispano, vamos a detenernos un poco más en ella, y a lo largo del texto, iremos remarcando algunos aspectos adicionales que consideramos deberían incluirse para que nuestro análisis de riesgo se enfoque un poco más a la resiliencia de la organización.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (CSAE) (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

CSAE: Consejo Superior de Administración Electrónica.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Derechos de utilización.

MAGERIT es una metodología de carácter público, puede ser utilizada libremente y no requiere autorización previa. En cualquier explotación de la obra se hará constar la autoría original.

En los próximo párrafos, iremos presentado textualmente las partes que nos interesan en este capítulo. Para que no quepa lugar a confusión, los párrafos tomados de la metodología se presentan en "*cursiva y color gris*", los comentarios que vayamos haciendo sobre la misma se mantendrán con el estilo de letra normal de todo este libro.

A lo largo de los siguientes capítulos, profundizaremos en el tema del análi*sis* de riesgo e iremos desarrollando casos prácticos, pero en lo que sigue a continuación, únicamente deseamos presentar brevemente la metodología MAGERIT, y la lógica de su implementación.

MAGERIT responde a lo que se denomina "Proceso de Gestión de Riesgos", aconsejando que suele ser prudente una aproximación iterativa, aplicando el método primero con "trazo grueso" y luego ir revisando el modelo para entrar en detalles, tratando de forma urgente los riesgos críticos , pudiendo ir tratando progresivamente los riesgos de menor criticidad. Entiéndase pues Magerit como una guía que se puede y se debe adaptar al caso y sus circunstancias.

En el punto 2. Visión de conjunto, establece que:

Hay dos grandes tareas a realizar:

I. análisis de riesgos,

que permite determinar qué tiene la Organización y estimar lo que podría pasar.

II. tratamiento de los riesgos,

que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

El análisis de riesgos considera los siguientes elementos:

1. *activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización*
2. *amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización*
3. *salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.*

Con estos elementos se puede estimar:

1. *el impacto: lo que podría pasar*
2. *el riesgo: lo que probablemente pase*

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

3. Método de análisis de riesgos

3.1.1. Paso 1: Activos (dependencias, valoración, dimensiones)

3.1.2. Paso 2: Amenazas (Identificación, valoración)

3.1.3. Determinación del impacto potencial

3.1.4. Determinación del riesgo potencial

3.1.5. Paso 3: Salvaguardas

3.1.6. Paso 4: impacto residual

3.1.7. Paso 5: riesgo residual

3.2. Formalización de las actividades

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

***MAR** – Método de Análisis de Riesgos*

MAR.1 – Caracterización de los activos

MAR.11 – Identificación de los activos

MAR.12 – Dependencias entre activos

MAR.13 – Valoración de los activos

MAR.2 – Caracterización de las amenazas

MAR.21 – Identificación de las amenazas

MAR.22 – Valoración de las amenazas

MAR.3 – Caracterización de las salvaguardas

MAR.31 – Identificación de las salvaguardas pertinentes

MAR.32 – Valoración de las salvaguardas

MAR.4 – Estimación del estado de riesgo

MAR.41 – Estimación del impacto

MAR.42 – Estimación del riesgo

4. Proceso de gestión de riesgos

A la vista de los impactos y riesgos a los que está expuesto el sistema, hay que tomar una serie de decisiones.

Todas las consideraciones desembocan en una calificación de cada riesgo significativo, determinándose si ...

1. *es **crítico** en el sentido de que requiere atención urgente*
2. *es **grave** en el sentido de que requiere atención*
3. *es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento*
4. *es **asumible** en el sentido de que no se van a tomar acciones para atajarlo*

El resultado del análisis es sólo un análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger y qué hemos hecho por protegerlo.

A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

- *paso 1: evaluación*
- *paso 2: tratamiento*

4.1.1. Evaluación: interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

4.1.2. Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la

responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios.

4.1.3. Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- *reducir el riesgo residual (aceptar un menor riesgo)*
- *ampliar el riesgo residual (aceptar un mayor riesgo)*

4.1.4. Estudio cuantitativo de costes / beneficios

Es de sentido común que no se puede invertir en salvaguardas más allá del valor que queremos proteger.

4.1.5. Estudio cualitativo de costes / beneficios

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

- *— aspectos reputacionales o de imagen*
- *— aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad*
- *— cumplimiento normativo, que puede ser obligatorio o voluntario*
- *— capacidad de operar*
- *— productividad*

4.1.7. Opciones de tratamiento del riesgo: eliminación

4.1.8. Opciones de tratamiento del riesgo: mitigación

4.1.9. Opciones de tratamiento del riesgo: compartición

4.1.10. Opciones de tratamiento del riesgo: financiación

4.2.7. Seguimiento y revisión

El análisis de los riesgos es un ejercicio formal, basado en múltiples estimaciones y valoraciones que pueden no compadecerse con la realidad. Es absolutamente necesario que el sistema esté bajo monitorización permanente. Los indicadores de impacto y riesgo potenciales son útiles para decidir qué puntos deben ser objeto de monitorización.

Hasta aquí hemos presentado, desde un punto de vista teórico, solamente los aspectos fundamentales de aplicar una metodología como es MAGERIT, en un proceso coherente y una secuencia de pasos a tener en cuenta. En los capítulos siguientes iremos viendo cómo hacerlo de forma práctica y aplicado a casos y situaciones reales, para seguir avanzando en nuestro objetivo de lograr tener redes y sistemas resilientes.

7. Análisis de Resiliencia en Redes y Sistemas.

Tal cual nos propone MAGERIT, vamos a iniciar este proceso iterativo del ciclo de vida de un análisis de riesgo, aplicando el método con "*trazo grueso, identificando y tratando urgentemente los riesgos críticos, pudiendo ir tratando progresivamente riesgos de menor criticidad*".

Tomemos por ejemplo una organización típica hoy en día, cuya estrategia de mercado radica en el número de subscriptores y el tratamiento (o algoritmia) que aplica sobre los mismos. Para que no nos quepa duda de lo que estamos hablando, el ejemplo propuesto es cualquier empresa que nos invita a que nos registremos para ofrecernos un servicio gratuito (Google, Facebook, Whatsapp, Instagram, etc.), por supuesto en una escala acorde a nuestras organizaciones.

Me interesa especialmente que avancemos sobre este ejemplo, pues podremos tomar como punto de partida, lo que venimos expresando durante todo el libro, la "Información". Nadie puede dudar que este tipo de empresa vive gracias a este preciado bien, y sobre el mismo monta toda su infraestructura ("***lo crítico es la Información… no las infraestructuras***").

Iniciemos con la metodología MAGERIT.

Paso 1: Activos (Ejemplo).

Paso 1 : Activos			
[info]			
	[vr1]		Algoritmos estadísticos
	[vr2]		Información de I+D
	[vr3]		Estrategias comerciales y financieras
	[per1]	[M]	Empleados
	[per2]	[A]	Clientes y partners
	[clasif]	[C]	Inteligencia de mercado
[ser]	[app]		Aplicación cliente
	[gest]		Gestión de sus plataformas

Podemos ir conformando una plantilla con la totalidad de los mismos, siguiendo el planteamiento inicial de adoptar un punto de partida con "trazo

grueso" pues lo que estamos haciendo es dar comienzo al primer ciclo de vida de esta actividad, se trata de comenzar a darle forma. Para mantenernos en la metodología MAGERIT, por ejemplo se puede comenzar a darle forma con la propuesta de activos del "catálogo" de la misma. A continuación se presenta un ejemplo de esta plantilla.

3	TIPOS DE ACTIVOS	
4	[S] Servicios	
5		[anon] anónimo (sin requerir identificación del usuario)
6		[pub] al público en general (sin relación contractual)
7		[ext] a usuarios externos (bajo una relación contractual)
8		[int] interno (usuarios y medios de la propia organización)
9		[cont] contratado a terceros (se presta con medios ajenos)
10		[www] world wide web
11		[telnet] acceso remoto a cuenta local
12		[email] correo electrónico
13		[file] almacenamiento de ficheros
14		[ftp] transferencia de ficheros
15		[edi] intercambio electrónico de datos
16		[dir] servicio de directorio
17		[idm] gestión de identidades
18		[ipm] gestión de privilegios
19		[pki] PKI - infraestructura de clave pública
20	[D] Datos / Información	
21		[files] ficheros
22		[password] credenciales (ej. Contraseñas)
23		[auth] datos de validación de credenciales
24		[acl] datos de control de acceso
25		[vr] datos vitales (vital records)
26		[com] datos de interés comercial
27		[adm] datos de interés para la administración pública
28		[int] datos de gestión interna
29		[voice] voz
30		[multimedia] multimedia
31		[source] código fuente
32		[exe] código ejecutable
33		[conf] datos de configuración
34		[log] registro de actividad (log)
35		[test] datos de prueba
36		[per] datos de carácter personal
37		[A] de nivel alto
38		[M] de nivel medio
39		[B] de nivel básico
40		[label] datos clasificados
41		[S] secreto
42		[R] reservado
43		[C] confidencial
44		[DL] difusión limitada
45		[SC] sin clasificar

46	[SW] Aplicaciones (software)	
47		[prp] desarrollo propio (in house)
48		[sub] desarrollo a medida (subcontratado)
49		[std] estándar (off the shelf)
50		[browser] navegador web
51		[www] servidor de presentación
52		[app] servidor de aplicaciones
53		[email_client] cliente de correo electrónico
54		[file] servidor de ficheros
55		[dbms] sistema de gestión de bases de datos
56		[tm] monitor transaccional
57		[office] ofimática
58		[av] anti virus
59		[os] sistema operativo
60		[ts] servidor de terminales
61		[backup] sistema de backup
62	[HW] Equipos informáticos (hardware)	
63		[host] grandes equipos
64		[mid] equipos medios
65		[pc] informática personal
66		[mobile] informática móvil
67		[pda] agendas electrónicas
68		[easy] fácilmente reemplazable
69		[data] que almacena datos
70		[peripheral] periféricos
71		[print] medios de impresión
72		[scan] escáneres
73		[crypto] dispositivos criptográficos
74		[network] soporte de la red
75		[modem] módems
76		[hub] concentradores
77		[switch] conmutadores
78		[router] encaminadores
79		[bridge] pasarelas
80		[firewall] cortafuegos
81		[wap] punto de acceso wireless
82		[pabx] centralita telefónica

83	[COM] Redes de comunicaciones	
84		[PSTN] red telefónica
85		[ISDN] rdsi (red digital)
86		[X25] X25 (red de datos)
87		[ADSL] ADSL
88		[pp] punto a punto
89		[radio] red inalámbrica
90		[sat] por satélite
91		[LAN] red local
92		[MAN] red metropolitana
93		[Internet] Internet
94		[vpn] red privada virtual
95	[SI] Soportes de información	
96		[electronic] electrónicos
97		[disk] discos
98		[san] almacenamiento en red
99		[cd] cederrón (CD-ROM)
100		[usb] dispositivos USB
101		[dvd] DVD
102		[tape] cinta magnética
103		[non_electronic] no electrónicos
104		[printed] material impreso
105		[tape] cinta de papel
106		[film] microfilm
107	[AUX] Equipamiento auxiliar	
108		[power] fuentes de alimentación
109		[ups] sistemas de alimentación ininterrumpida
110		[gen] generadores eléctricos
111		[ac] equipos de climatización
112		[cabling] cableado
113		[robot] robots
114		[tape] ... de cintas
115		[disk] ... de discos
116		[supply] suministros esenciales
117		[destroy] equipos de destrucción de soportes de información
118		[furniture] mobiliario: armarios, etc
119		[safe] cajas fuertes
120	[L] Instalaciones	
121		[site] emplazamiento
122		[building] edificio
123		[local] local
124		[mobile] plataformas móviles
125		[car] vehículo terrestre: coche, camión, etc.
126		[plane] vehículo aéreo: avión, etc.
127		[ship] vehículo marítimo: buque, lancha, etc.
128		[shelter] contenedores
129		[channel] canalización
130	[P] Personal	
131		[ue] usuarios externos
132		[ui] usuarios internos
133		[op] operadores
134		[adm] administradores de sistemas
135		[com] administradores de comunicaciones
136		[dba] administradores de BBDD
137		[des] desarrolladores
138		[sub] subcontratas
139		[prov] proveedores

Siguiendo la lógica de MAGERIT deberíamos poder valorar los activos sobre los que podamos hacerlo, reiteramos que este es el punto de partida, por lo que, para ser prácticos, hagamos una primera aproximación, intentando que sea lo más precisa posible, pero NO perfecta, ya tendremos muchos ciclos de vida más para ajustarla. A continuación presentamos una primera aproximación como ejemplo.

En la plantilla podemos apreciar un valor aproximado de lo que se estima para cada activo. Hemos intentado remarcar o poner especial interés en la importancia de la "Información" sobre los activos asociados a infraestructura.

Un aspecto muy importante que pone de manifiesto MAGERIT son las dependencias. No podemos considerar los activos de forma aislada, pues justamente lo que estamos trabajando es poder determinar que riesgo tiene mi organización en su conjunto, y el mismo será la suma de las partes, por lo que si una parte sufre un incidente y este impacta en otra parte de la organización, no se trata de un hecho aislado sino de una concatenación de los mismos. El ejemplo más claro en estos casos es la caída de un servidor, o un disco duro, o de la red, cualquiera de ellos dejará fuera de servicio, la información que almacena o la que transita por ella, por lo que es necesario

Nº	Activo	Valoración
1	[files] ficheros	50.000 €
2	[vr] datos vitales (vital records)	80.000 €
3	[com] datos de interés comercial	10.000 €
4	[source] código fuente	5000 €
5	[prp] desarrollo propio (in house)	35.000 €
6	[sub] desarrollo a medida (subcontratado)	5000 €
7	[www] servidor de presentación	5000 €
8	[app] servidor de aplicaciones	10.000 €
9	[file] servidor de ficheros	10.000 €
10	[dbms] sistema de gestión de bases de dat	40.000 €
11	[office] ofimática	10.000 €
12	[av] anti virus	2000 €
13	[os] sistema operativo	2000 €
14	[ts] servidor de terminales	1000 €
15	[backup] sistema de backup	40.000 €
16	[host] grandes equipos	40.000 €
17	[mid] equipos medios	10.000 €
18	[pc] informática personal	5000 €
19	[mobile] informática móvil	2000 €
20	[peripheral] periféricos	5000 €
21	[print] medios de impresión	2000 €
22	[scan] escáneres	1000 €
23	[network] soporte de la red	10.000 €
24	[router] encaminadores	10.000 €
25	[switch] conmutadores	5000 €
26	[firewall] cortafuegos	10.000 €
27	[wap] punto de acceso wireless	2000 €
28	[pabx] centralita telefónica	1000 €
29	[PSTN] red telefónica	1000 €
30	[ISDN] rdsi (red digital)	1000 €
31	[vpn] red privada virtual	2000 €
32	[disk] discos	10.000 €
33	[san] almacenamiento en red	10.000 €
34	[power] fuentes de alimentación	5000 €
35	[ac] equipos de climatización	10.000 €
36	[cabling] cableado	5000 €
37	[supply] suministros esenciales	3000 €
38	[furniture] mobiliario: armarios, etc	5000 €
39	[safe] cajas fuertes	1000 €
40	[car] vehículo terrestre: coche, camión, etc.	20.000 €
41	[site] emplazamiento	5000 €
	Total:	**354.000 €**

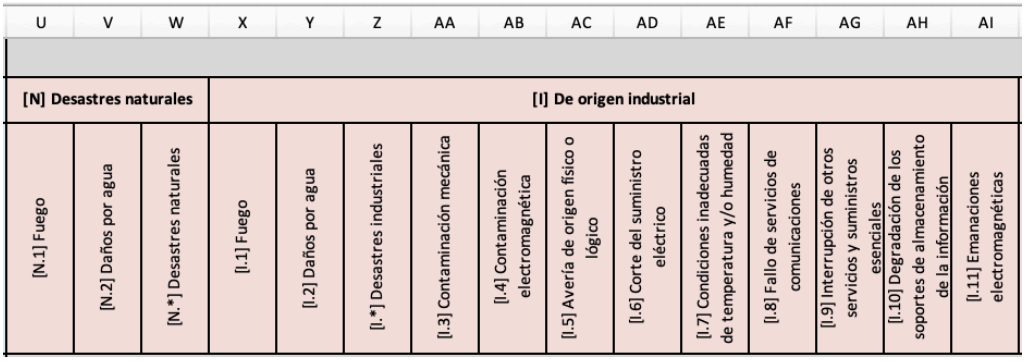
ahora poder determinar esta grados de dependencia, o relación entre estos recursos, nuevamente ponemos un ejemplo a continuación.

Nº	Activo	Valoración	Dependencias
1	[files] ficheros	50.000 €	4,5,9,12,16,26,32,33,34
2	[vr] datos vitales (vital records)	80.000 €	1,10,15
3	[com] datos de interés comercial	10.000 €	1,10,15
4	[source] código fuente	5000 €	1,10,15
5	[prp] desarrollo propio (in house)	35.000 €	1
6	[sub] desarrollo a medida (subcontratado)	5000 €	1
7	[www] servidor de presentación	5000 €	16,17
8	[app] servidor de aplicaciones	10.000 €	10,16,17
9	[file] servidor de ficheros	10.000 €	1,16,17
10	[dbms] sistema de gestión de bases de datos	40.000 €	15,16,17
11	[office] ofimática	10.000 €	12,13,18
12	[av] anti virus	2000 €	16,17
13	[os] sistema operativo	2000 €	12,15
14	[ts] servidor de terminales	1000 €	23
15	[backup] sistema de backup	40.000 €	5,16,32
16	[host] grandes equipos	40.000 €	
17	[mid] equipos medios	10.000 €	
18	[pc] informática personal	5000 €	11,13
19	[mobile] informática móvil	2000 €	11,13
20	[peripheral] periféricos	5000 €	
21	[print] medios de impresión	2000 €	
22	[scan] escáneres	1000 €	
23	[network] soporte de la red	10.000 €	
24	[router] encaminadores	10.000 €	23,36
25	[switch] conmutadores	5000 €	23,36
26	[firewall] cortafuegos	10.000 €	23,36
27	[wap] punto de acceso wireless	2000 €	23,36
28	[pabx] centralita telefónica	1000 €	36
29	[PSTN] red telefónica	1000 €	36
30	[ISDN] rdsi (red digital)	1000 €	36
31	[vpn] red privada virtual	2000 €	23,24,26
32	[disk] discos	10.000 €	4,16
33	[san] almacenamiento en red	10.000 €	23,24,26,32
34	[power] fuentes de alimentación	5000 €	
35	[ac] equipos de climatización	10.000 €	
36	[cabling] cableado	5000 €	
37	[supply] suministros esenciales	3000 €	
38	[furniture] mobiliario: armarios, etc	5000 €	
39	[safe] cajas fuertes	1000 €	
40	[car] vehículo terrestre: coche, camión, etc.	20.000 €	
41	[site] emplazamiento	5000 €	
	Total:	**354.000 €**	

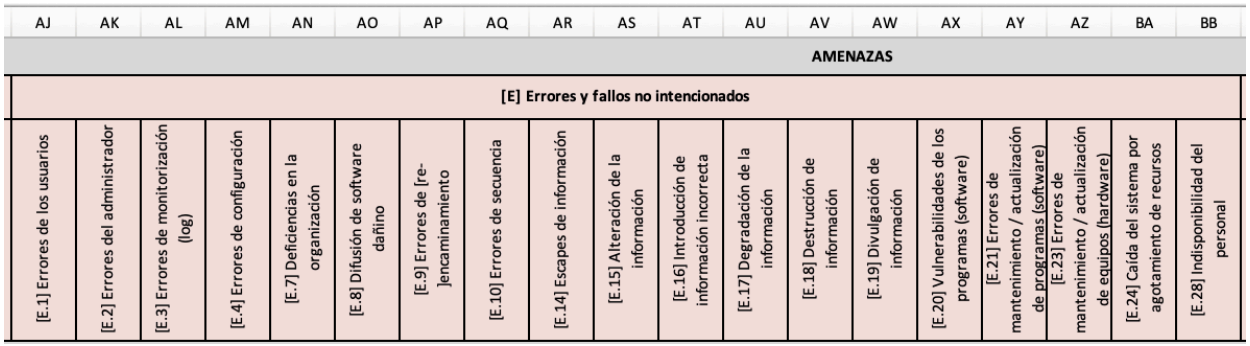
Paso 2: Amenazas (Ejemplo).

Sigamos avanzando, ahora en el análisis de las amenazas. Para ir organizando los cálculos y facilitar el seguimiento de un verdadero ciclo de

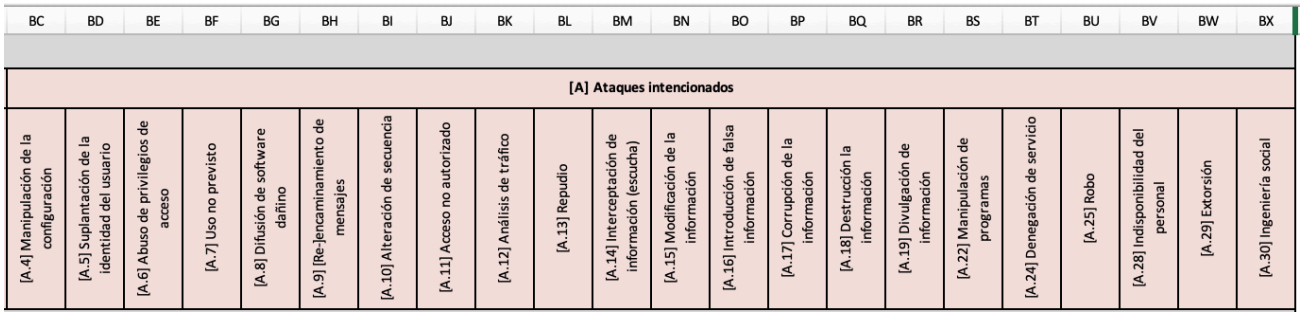
vida, mantendremos este diseño en forma de plantilla, por lo que a continuación presentamos un ejemplo de cómo podríamos ir organizando la misma.



U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
[N] Desastres naturales			[I] De origen industrial											
[N.1] Fuego	[N.2] Daños por agua	[N.*] Desastres naturales	[I.1] Fuego	[I.2] Daños por agua	[I.*] Desastres industriales	[I.3] Contaminación mecánica	[I.4] Contaminación electromagnética	[I.5] Avería de origen físico o lógico	[I.6] Corte del suministro eléctrico	[I.7] Condiciones inadecuadas de temperatura y/o humedad	[I.8] Fallo de servicios de comunicaciones	[I.9] Interrupción de otros servicios y suministros esenciales	[I.10] Degradación de los soportes de almacenamiento de la información	[I.11] Emanaciones electromagnéticas

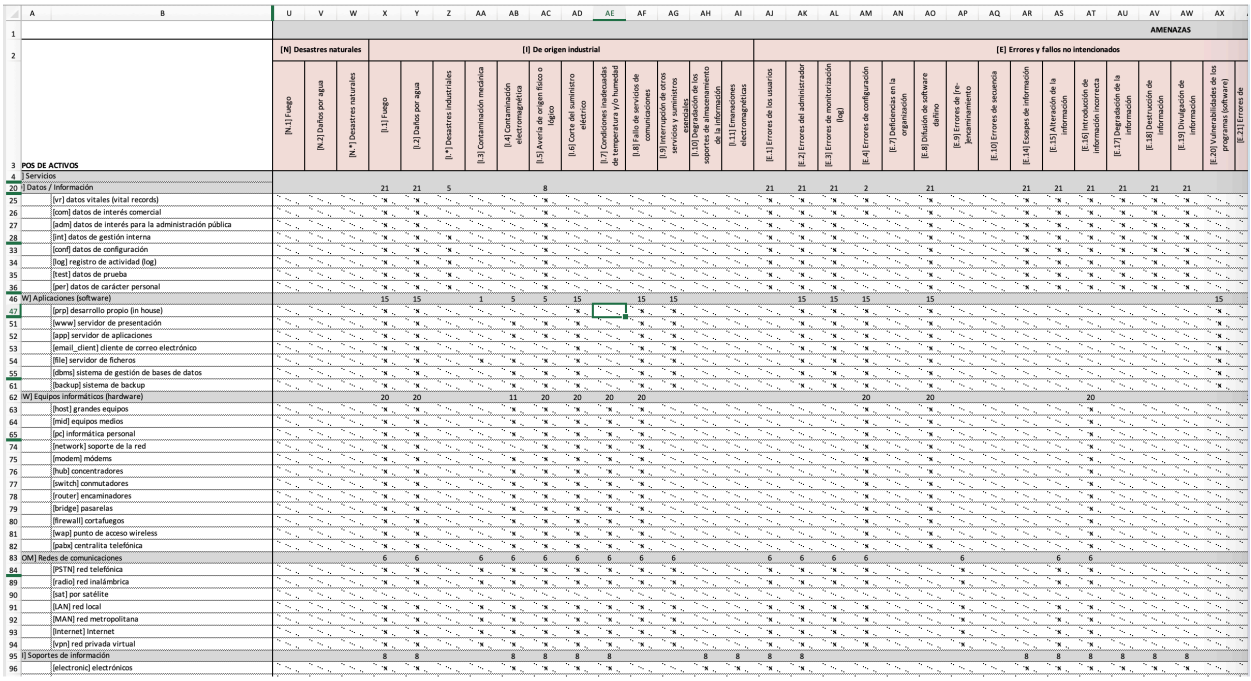


AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB
AMENAZAS																		
[E] Errores y fallos no intencionados																		
[E.1] Errores de los usuarios	[E.2] Errores del administrador	[E.3] Errores de monitorización (log)	[E.4] Errores de configuración	[E.7] Deficiencias en la organización	[E.8] Difusión de software dañino	[E.9] Errores de [re-]encaminamiento	[E.10] Errores de secuencia	[E.14] Escapes de información	[E.15] Alteración de la información	[E.16] Introducción de información incorrecta	[E.17] Degradación de la información	[E.18] Destrucción de información	[E.19] Divulgación de información	[E.20] Vulnerabilidades de los programas (software)	[E.21] Errores de mantenimiento / actualización de programas (software)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[E.24] Caída del sistema por agotamiento de recursos	[E.28] Indisponibilidad del personal



BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV	BW	BX
[A] Ataques intencionados																					
[A.4] Manipulación de la configuración	[A.5] Suplantación de la identidad del usuario	[A.6] Abuso de privilegios de acceso	[A.7] Uso no previsto	[A.8] Difusión de software dañino	[A.9] [Re-]encaminamiento de mensajes	[A.10] Alteración de secuencia	[A.11] Acceso no autorizado	[A.12] Análisis de tráfico	[A.13] Repudio	[A.14] Interceptación de información (escucha)	[A.15] Modificación de la información	[A.16] Introducción de falsa información	[A.17] Corrupción de la información	[A.18] Destrucción la información	[A.19] Divulgación de información	[A.22] Manipulación de programas	[A.24] Denegación de servicio	[A.25] Robo	[A.28] Indisponibilidad del personal	[A.29] Extorsión	[A.30] Ingeniería social

Una vez identificadas las amenazas, debemos continuar evaluando cómo aplican cada una de ellas sobre los recursos que ya tenemos en nuestra plantilla de cálculo. En nuestro caso, solamente hemos decidido verificar su correspondencia, es decir "aplica" o "no aplica", pero por supuesto que se trata de una decisión particular, en la que cada uno puede poner los umbrales que desee y valorarlos con el detalle que crea conveniente. A continuación presentamos un ejemplo de cómo podría hacerse (se han ocultado varias filas, para que pueda apreciarse la imagen, de forma más global).



Como se puede apreciar en la imagen anterior, el cruce de cada fila que aplica con su amenaza correspondiente, va generando las sumatorias globales para poder obtener resultados con máximo detalle a nivel individual o grupal.

En nuestro caso particular, siempre nos ha parecido necesario realizar una primera aproximación para relacionar estos activos que ya tenemos trabajados en relación a los riesgos que sabemos que tienen de forma "intrínseca" o inicial. Por tratarse de una empresa, que como hemos propuesto al inicio del capítulo, opera sobre datos de clientes, en este ejemplo hemos identificado dos clases de riesgos iniciales "generales" (que como se puede apreciar, guardan relación con las "dimensiones" de MAGERIT" y datos personales, pues sabemos que es el mayo riesgo que enfrentamos.

Esta primera aproximación, a diferencia de las amenazas, sí hemos decidido asignarles una valor, peso o importancia que consideramos aplicada uno de ellos en relación a cada activo. Como podéis apreciar hemos decidido asignarle una escala de 0 a 3 y N/A (No Aplica).

A continuación presentamos la imagen.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1			RIESGOS																	
2			GENERALES							PROTECCION DE DATOS										
3	TIPOS DE ACTIVOS		[D] disponibilidad	[I] integridad de los datos	[C] confidencialidad de los datos	[A_S] autenticidad de los usuarios del servicio	[A_D] autenticidad del origen de los datos	[T_S] trazabilidad del servicio	[T_D] trazabilidad de los datos	Generales / reputacionales	Legitimación de los tratamientos y cesiones de DCP	Transferencias Internacionales	Notificación de los tratamientos	Transparencia de los tratamientos	Calidad de los datos	Datos especialmente protegidos	Deber de secreto	Tratamientos por encargo	Derechos del afectado	Seguridad
4	[S] Servicios		1,5	1,7	2,2	2,0	1,9	2,1	2,0	1,5	1,6	0,0	1,2	1,2	1,4	1,5	1,5	1,4	1,3	1,5
20	[D] Datos / Información		2,3	2,2	2,2	2,2	2,2	2,1	2,1	2,1	2,2	0,0	1,9	1,6	2,2	2,1	2,1	2,1	2,1	2,2
25		[vr] datos vitales (vital records)	3	3	3	3	3	3	3	3	3	N/A	3	2	3	3	3	3	3	3
26		[com] datos de interés comercial	1	1			1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
27		[adm] datos de interés para la administración pública	2	3			3	2	2	3	3	N/A	3	2	3	3	3	3	3	3
28		[int] datos de gestión interna	2	2			3	2	2	2	2	N/A	3	2	3	3	3	3	3	3
33		[conf] datos de configuración	3	2			2	2	2	2	2	N/A	1	1	2	3	3	3	3	3
34		[log] registro de actividad (log)	3	2			3	3	3	3	3	N/A	2	2	3	3	3	3	3	3
35		[test] datos de prueba	1	1			1	1	1	1	1	N/A	1	1	3	2	2	2	2	3
36		[per] datos de carácter personal	3	3			3	3	3	3	3	N/A	3	2	3	3	3	3	3	3
46	[SW] Aplicaciones (software)		1,8	2,3			1,7	1,6	1,3	1,3	1,3	0,0	1,3	1,3	1,5	3,0	1,4	1,3	1,3	3,0
47		[prp] desarrollo propio (in house)	0	2	1	1	1	1	1	1	1	N/A	1	1	1	3	2	1	1	3
51		[www] servidor de presentación	1	2	1	1	1	1	1	1	1	N/A	1	1	1	3	1	1	1	3
52		[app] servidor de aplicaciones	3	2	1	1	1	1	1	1	1	N/A	1	1	1	3	1	1	1	3
53		[email_client] cliente de correo electrónico	1	2	2	3	2	2	1	1	1	N/A	1	1	1	3	1	1	1	3
54		[file] servidor de ficheros	3	3	3	3	2	2	2	2	2	N/A	2	2	2	3	2	2	2	3
55		[dbms] sistema de gestión de bases de datos	3	3	3	3	3	2	2	2	2	N/A	2	2	2	3	2	2	2	3
61		[backup] sistema de backup	3	2	2	3	2	2	2	2	2	N/A	2	2	2	3	2	2	2	3
62	[HW] Equipos informáticos (hardware)		0,6	1,1	2,1	1,6	1,3	1,4	1,3	1,1	1,1	0,0	1,3	1,3	1,3	1,3	1,3	1,3	1,3	1,3
63		[host] grandes equipos	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
64		[mid] equipos medios	2	1	2	3	1	2	1	1	1	N/A	2	2	2	2	2	2	2	2
65		[pc] informática personal	2	2	3	3	2	2	2	2	2	N/A	3	3	3	3	3	3	3	3
74		[network] soporte de la red	1	1	2	2	2	2	2	1	1	N/A	1	1	1	1	1	1	1	1
75		[modem] módems	0	1	2	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
76		[hub] concentradores	0	1	2	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
77		[switch] conmutadores	0	1	2	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
78		[router] encaminadores	0	1	1	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
79		[bridge] pasarelas	0	1	1	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
80		[firewall] cortafuegos	1	1	2	2	2	2	2	1	1	N/A	1	1	1	1	1	1	1	1
81		[wap] punto de acceso wireless	0	1	2	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
82		[pabx] centralita telefónica	0	1	2	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
83	[COM] Redes de comunicaciones		1,0	1,8	2,7	2,7	2,7	2,0	2,0	2,0	2,0	0,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0
84		[PSTN] red telefónica	1	1	1	1	1	1	1	1	1	N/A	1	1	1	1	1	1	1	1
89		[radio] red inalámbrica	1	2	3	3	3	3	3	3	3	N/A	3	3	3	3	3	3	3	3
90		[sat] por satélite	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
91		[LAN] red local	1	2	3	3	3	2	2	2	2	N/A	2	2	2	2	2	2	2	2
92		[MAN] red metropolitana	1	2	3	3	3	2	2	2	2	N/A	2	2	2	2	2	2	2	2
93		[Internet] Internet	1	2	3	3	3	2	2	2	2	N/A	2	2	2	2	2	2	2	2
94		[vpn] red privada virtual	1	2	3	3	3	2	2	2	2	N/A	2	2	2	2	2	2	2	2
95	[SI] Soportes de información		2,3	2,6	3,0	3,0	3,0	3,0	3,0	3,0	3,0	0,0	2,0	2,0	3,0	3,0	3,0	3,0	3,0	3,0
96		[electronic] electrónicos	2	3	3	3	3	3	3	3	3	N/A	2	2	3	3	3	3	3	3

3
2
1
0
N/A

Como en el caso anterior, también en las filas color "gris" va acumulando los promedios de cada uno de los grupos de activos.

Paso 3: Salvaguardas (Ejemplo).

Siguiendo los pasos de MAGERIT, lo que nos toca trabajar ahora son las salvaguardas. Siguiendo con el ejemplo de nuestra empresa, nuevamente ponemos especial atención en el tema de los datos de clientes, por lo que la protección de datos es fundamental. Para esta tarea tomamos como referencia el **Reglamento General de Protección de Datos** de la Unión Europea (**RGPD**), en el caso de España, la Agencia Española de Protección de Datos (https://www.aepd.es/es), viene haciendo un trabajo excelente en

cuanto a guías y manuales de referencia, de las mismas podemos obtener la gran mayoría de las líneas de las imágenes que presentamos a continuación.

2	**SALVAGUARDAS EN LA PROTECCION DE DATOS**									
3	**ANÁLISIS DE CUMPLIMIENTO NORMATIVO**									
4	Uno de los aspectos decisivos en toda Evaluación de Impacto en la Protección de Datos (EIPD) es el relativo a la verificación de la conformidad del proyecto con las distintas regulaciones que pueden contener elementos relativos a la privacidad y a la protección de datos que le sean de aplicación. Ello incluye la legislación básica de protección de datos personales y, en concreto, la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo. Pero, dependiendo del sector en el que opere la organización o del proyecto concreto, también pueden existir obligaciones adicionales como, por ejemplo, la legislación sanitaria, de telecomunicaciones o de servicios de sociedad de la información o, en la propia LOPD, lo que se refiere a los ficheros de las Fuerzas y Cuerpos de Seguridad, a la prestación de servicios de solvencia patrimonial y crédito, o los tratamientos con fines de publicidad y prospección comercial. Para facilitar la realización de este análisis, a continuación, se detalla una guía en la que se incluyen una serie de cuestiones a las que sería necesario dar respuesta para comprobar si los tratamientos de datos personales que estamos analizando respetan los principios y derechos establecidos, sin abordar la revisión de otras normas que pudieran resultar de									
6	**Legitimación de los tratamientos y las cesiones de datos personales**	**RESPUESTA**	**[S]**	**[D]**	**[SW]**	**[HW]**	**[COM]**	**[SI]**	**[AUX]**	**[L]**	**[P]**
7	¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para el tratamiento de sus datos personales?	SI		SI							SI
8	En caso contrario, ¿se da alguna de las siguientes circunstancias?	N/A		N/A							N/A
28	¿Se han habilitado procedimientos para gestionar la revocación del consentimiento del afectado?	SI		SI							SI
30	**Transferencias internacionales**	**RESPUESTA**	**[S]**	**[D]**	**[SW]**	**[HW]**	**[COM]**	**[SI]**	**[AUX]**	**[L]**	**[P]**
31	¿Se van a transferir datos personales fuera de España?	N/A		N/A							
38	**Notificación de los tratamientos a la AEPD**	**RESPUESTA**	**[S]**	**[D]**	**[SW]**	**[HW]**	**[COM]**	**[SI]**	**[AUX]**	**[L]**	**[P]**
39	¿Se han seguido los pasos necesarios para notificar al Registro General de Protección de Datos de la AEPD los ficheros o tratamientos de datos personales?	SI		SI							
40	En el caso de que el responsable sea una Administración Pública, ¿se ha publicado la disposición de carácter general en el diario oficial correspondiente?	N/A		N/A							
42	**Transparencia de los tratamientos**	**RESPUESTA**	**[S]**	**[D]**	**[SW]**	**[HW]**	**[COM]**	**[SI]**	**[AUX]**	**[L]**	**[P]**
43	¿Se informa a los afectados expresa e inequívocamente de la existencia de un tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios de los datos, de la obligatoriedad o no de las respuestas y de las consecuencias de no prestarlas y de la posibilidad de ejercer los derechos del afectado?	SI		SI							
44	¿Figura la anterior información en los formularios, tradicionales o electrónicos, de recogida de información?	SI		SI							
45	Si los datos no se recaban directamente de los afectados, ¿se informa a los mismos, en el plazo de tres meses desde el registro de los datos personales, de forma expresa e inequívoca de la existencia de un tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios de los datos y de la posibilidad de ejercer los derechos del afectado?	N/A		N/A							
47	**Calidad de los datos**	**RESPUESTA**	**[S]**	**[D]**	**[SW]**	**[HW]**	**[COM]**	**[SI]**	**[AUX]**	**[L]**	**[P]**
	¿Se definen los plazos de conservación de los datos personales? ¿Existen procedimientos para determinar que se han cumplido los plazos máximos de	NO		NO							

Datos especialmente protegidos	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
Si se tratan datos especialmente protegidos de ideología, religión, creencias o afiliación sindical, ¿se cuenta con el consentimiento expreso y por escrito?	SI		SI							
Si se tratan datos especialmente protegidos de salud, vida sexual u origen racial o étnico, ¿se cuenta con el consentimiento expreso? En caso contrario, ¿existe una ley que permita su tratamiento?	N/A		N/A							

Deber de secreto	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
¿Se forma adecuadamente a todas las personas que tratan datos de carácter personal de la obligación de guardar secreto sobre los datos que conozcan en el ejercicio de sus funciones?	SI									SI
¿Se les informa adecuadamente de sus obligaciones y de las consecuencias de no hacerlo? ¿Queda constancia de dicha información?	SI									SI

Tratamientos por encargo	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
¿Se han realizado los análisis necesarios de manera diligente para elegir un encargado de tratamiento que ofrezca las garantías adecuadas?	SI		SI							
¿Se regula la relación entre el responsable y el encargado en un contrato (escrito o acordado electrónicamente con las garantías que establece la ley)?	SI		SI							

Derechos del afectado	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
¿Se adoptan las medidas necesarias para garantizar el carácter personalísimo (verificación de la identidad o, en su caso, de la validez de la representación otorgada a un tercero) del ejercicio de los derechos?	SI		SI							

SEGURIDAD

General	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
¿Se ha llevado a cabo la clasificación e identificación del nivel de seguridad (básico, medio o alto) que deben satisfacer todos y cada uno de los ficheros o tratamientos de datos personales?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
¿Se garantiza que las medidas de seguridad para el acceso a datos personales a través de redes de telecomunicaciones garantizan el mismo nivel de seguridad que el existente en el entorno local?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
¿Existe un procedimiento para gestionar las autorizaciones para la salida de dispositivos portátiles que contienen datos personales fuera de los locales del responsable?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
¿Cumplen las copias de trabajo y los ficheros temporales las medidas de seguridad correspondientes a su nivel? ¿Se destruyen una vez han dejado de ser necesarios?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
¿Se ha elaborado el preceptivo documento de seguridad (DS)?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Seguridad ficheros automatizados

Nivel Básico	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
¿Se han definido claramente en el DS las funciones y obligaciones de los usuarios que acceden a los sistemas de información que contienen datos personales?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
¿Se han establecido los procedimientos necesarios para que todo el personal conozca las medidas de seguridad que le afectan y que debe implantar?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

	Nivel Medio (además de las del Nivel Básico):	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
129	¿Se ha designado un responsable o responsables de seguridad?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
130	¿Se realizan auditorías bienales o cada vez que se produzcan modificaciones sustanciales en los sistemas de información?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

	Nivel Alto (además de las del Nivel Básico y Medio):	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
137	¿Existen procedimientos y herramientas para cifrar los soportes durante su distribución fuera de los locales del responsable? ¿Y para los dispositivos portátiles?	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Seguridad ficheros manuales

	Nivel Básico	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
146	¿Se han definido criterios de archivo para garantizar la correcta conservación de los documentos, su localización, su consulta y el ejercicio de los derechos del afectado?	SI		SI						SI	SI
147	¿Los dispositivos de almacenamiento de documentos están dotados de mecanismos que dificulten su apertura?	SI		SI						SI	SI

	Nivel Medio	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
156	¿Se ha designado un responsable o responsables de seguridad?	SI		SI							SI
157	¿Se realizan auditorías bienales o cada vez que se produzcan modificaciones sustanciales en los sistemas de información?	SI		SI							SI

	Nivel Alto	RESPUESTA	[S]	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
160	¿Se conservan los armarios y archivadores en áreas separadas protegidos con puertas de acceso con llave u otro dispositivo equivalente?	SI		SI						SI	SI
166			2	4	2	2	2	2	2	2	2

Como en otras imágenes anteriores, también hemos ocultado alguna líneas para que no sean tan extensas las imágenes, pero si deseamos remarcar la importancia que tiene este análisis de salvaguardas relacionadas a los datos personales (en nuestro caso) pues si se presta atención se puede ver que son 166 líneas las que se ponderan en esta actividad.

En las imágenes anteriores se pone de manifiesto también que cada una de las líneas de salvaguardas, se las valora y relaciona con todos los grupos de activos que ya hemos procesado ([S], [D], [W]…etc.).

Otro aspecto relacionado con las salvaguardas que también debemos considerar son el conjunto de medidas técnicas que están a mi alcance. También presentamos a continuación las imágenes correspondientes.

SALVAGUARDAS TÉCNICAS	
Las salvaguardas permiten hacer frente a las amenazas. Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:	

GENERAL	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
Organización de la seguridad: roles, comités, ...	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Política corporativa de seguridad de la información	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestión de privilegios: adjudicación, revisión y terminación	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Procedimientos de escalado y gestión de incidencias	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Procedimientos de continuidad de operaciones: emergencia y recuperación	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Auditoría, registro (certificación) y acreditación del sistema	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

PROTECCIÓN DE LOS SERVICIOS	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
Especificación del servicio	SI	SI				SI				
Desarrollo del servicio	SI	SI				SI				
Despliegue del servicio	SI	SI				SI				
Operación del servicio	SI	SI				SI				
Terminación del servicio	SI	SI				SI				

PROTECCIÓN DE LAS APLICACIONES (SOFTWARE)	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
Especificación funcional y no funcional	N/A			N/A						
Desarrollo seguro	N/A			N/A						
Protección del código fuente	N/A			N/A						
Aceptación y puesta en operación	N/A			N/A						
Explotación	N/A			N/A						
Gestión de cambios y configuración	N/A			N/A						
Gestión de incidencias	N/A			N/A						
Homologación / certificación / acreditación	N/A			N/A						

PROTECCIÓN DE LOS EQUIPOS (HARDWARE)	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
Seguridad física										
Inventario	SI			SI	SI	SI	SI	SI	SI	
Control de entradas y salidas	SI			SI	SI	SI	SI	SI	SI	
Destrucción	SI			SI	SI	SI	SI	SI	SI	
Homologación / certificación / acreditación	SI			SI	SI	SI	SI	SI	SI	
Seguridad del sistema operativo										
Configuración	SI			SI	SI	SI	SI	SI	SI	
Equipos internos	SI			SI	SI	SI	SI	SI	SI	
Equipos que salen de los locales	SI			SI	SI	SI	SI	SI	SI	
Mantenimiento:										
Protección frente a código dañino: virus, espías, etc.	SI			SI	SI	SI	SI	SI	SI	
Detección de intrusión	SI			SI	SI	SI	SI	SI	SI	
Registro de actuaciones	SI			SI	SI	SI	SI	SI	SI	
Gestión de privilegios	SI			SI	SI	SI	SI	SI	SI	
Control de acceso	SI			SI	SI	SI	SI	SI	SI	

	PROTECCIÓN DE LAS COMUNICACIONES	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
48	Planificación de capacidad	SI	SI				SI	SI	SI	SI	
49	Adquisición y mantenimiento	SI	SI				SI	SI	SI	SI	
50	Configuración	SI	SI				SI	SI	SI	SI	
51	Segregación de redes	SI	SI				SI	SI	SI	SI	
52	Configuración de routers	SI	SI				SI	SI	SI	SI	
53	Configuración de cortafuegos	SI	SI				SI	SI	SI	SI	
54	Gestión de claves, si se emplea cifrado	SI	SI				SI	SI	SI	SI	
55	Detección de intrusión	SI	SI				SI	SI	SI	SI	
56	Monitorización de uso	SI	SI				SI	SI	SI	SI	

	SEGURIDAD FÍSICA	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
59	Protección de las instalaciones										
60	Frente a accidentes naturales: terremotos, riadas, incendios, tormentas, etc.	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A	
61	Frente a accidentes industriales: incendio, inundación, etc.	SI	SI	SI		SI	SI	SI	SI	SI	
62	Contaminación mecánica: polvo, vibraciones	SI	SI	SI		SI	SI	SI	SI	SI	
63	Contaminación electromagnética	SI	SI	SI		SI	SI	SI	SI	SI	
64	Protección frente a emanaciones electromagnéticas	SI	SI	SI		SI	SI	SI	SI	SI	
65	Protección del recinto: edificios, locales y áreas de trabajo	SI	SI	SI		SI	SI	SI	SI	SI	
66	Anuncio mínimo	SI	SI	SI		SI	SI	SI	SI	SI	
67	Barreras físicas	SI	SI	SI		SI	SI	SI	SI	SI	
68	Protección del cableado	SI	SI	SI		SI	SI	SI	SI	SI	
69	Control de acceso: entrada y salida de personas, equipos, soportes de información, etc.	SI	SI	SI		SI	SI	SI	SI	SI	

	RELATIVAS AL PERSONAL	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
72	Especificación del puesto de trabajo	SI									SI
73	Selección de personal	SI									SI
74	Condiciones contractuales: responsabilidad en seguridad	SI									SI
75	Formación continua	SI									SI

	EXTERNALIZACIÓN	RESPUESTA	(S)	[D]	[SW]	[HW]	[COM]	[SI]	[AUX]	[L]	[P]
78	Desarrollo de aplicaciones o equipos	SI	SI	SI	SI	SI	SI	SI	SI	SI	
79	Aplicaciones que se ejecutan en otro lugar con acceso remoto (ASP – Application Service Provisioning)	SI	SI	SI	SI	SI	SI	SI	SI	SI	
80	Mantenimiento de programas y equipos	SI	SI	SI	SI	SI	SI	SI	SI	SI	
81	Seguridad gestionada: monitorización remota y gestión delegada de incidencias	SI	SI	SI	SI	SI	SI	SI	SI	SI	
82	Prestación de servicios de comunicaciones	SI	SI	SI	SI	SI	SI	SI	SI	SI	
83	Prestación de servicios de custodia de datos / información	SI	SI	SI	SI	SI	SI	SI	SI	SI	
84	…										
85	En todos estos casos es fundamental cerrar los aspectos de relación contractual: • SLA: nivel de servicio, si la disponibilidad es un valor • NDA: compromiso de secreto, si la confidencialidad es un valor • Identificación y calificación del personal encargado • Procedimientos de escalado y resolución de incidencias • Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas) • Asunción de responsabilidades y penalizaciones por incumplimiento										
86			0	0	0	0	0	0	0	0	0

Por último, si hemos seguido metodológicamente cada uno de los pasos, y realizado los cálculos necesarios lograremos tener una primera impresión de cómo es el nivel de riesgo que estoy planteando según este trabajo.

Nuevamente proponemos un ejemplo que puede ser el adecuado a la organización del lector, o no, pero lo importante del mismo es que es una línea de trabajo metódica, basada en MAGERIT que nos está ofreciendo una primera visión del problema. A continuación se presenta la imagen del ejemplo.

TIPOS DE ACTIVOS	RIESGOS GENERALES							RIESGOS DE PROTECCION DE DATOS										RIESGOS GENERALES	RIESGOS DE PROTECCION DE DATOS	IMPACTO DE AMENAZA	SALVAGUARDAS		RIESGO RESIDUAL
	[D] disponibilidad	[I] integridad de los datos	[C] confidencialidad de los datos	[A_S] autentidad de los usuarios del servicio	[A_D] autentidad del origen de los datos	[T_S] trazabilidad del servicio	[T_D] trazabilidad de los datos	Generales / reputacionales	Legitimación de los tratamientos y cesiones de DCP	Transferencias internacionales	Notificación de los tratamientos	Transparencia de los tratamientos	Calidad de los datos	Datos especialmente protegidos	Deber de secreto	Tratamientos por encargo	Derechos del afectado	Seguridad	Valoración	Valoración	Valoración	PROTECCIÓN DE DATOS	TÉCNICAS	
[S] Servicios	2	2	2	2	2	2	2	2	1	0	1	1	1	1	2	2	2	2	MEDIO	BAJO	BAJO	Satisfactorio	Satisfactorio	BAJO
[D] Datos / Información	2	2	2	2	2	2	2	2	1	0	1	1	1	1	2	2	2	2	MEDIO	MEDIO	ALTO	Satisfactorio	Satisfactorio	BAJO
[SW] Aplicaciones (software)	2	2	2	2	2	2	2	2	1	0	1	1	1	3	2	2	2	3	MEDIO	MEDIO	MEDIO	Satisfactorio	Satisfactorio	BAJO
[HW] Equipos informáticos (hardware)	2	1	1	1	1	2	2	2	1	0	1	1	1	1	2	2	2	2	BAJO	BAJO	ALTO	Satisfactorio	Satisfactorio	BAJO
[COM] Redes de comunicaciones	2	2	3	3	3	2	2	2	1	0	2	1	1	1	2	2	2	2	MEDIO	MEDIO	ALTO	Satisfactorio	Satisfactorio	BAJO
[SI] Soportes de información	2	3	3	3	3	3	3	2	1	0	2	1	1	1	3	3	3	3	ALTO	ALTO	MEDIO	Satisfactorio	Satisfactorio	BAJO
[AUX] Equipamiento auxiliar	1	1	1	1	1	2	2	2	1	0	1	1	1	1	2	2	2	2	BAJO	BAJO	MEDIO	Satisfactorio	Satisfactorio	BAJO
[L] Instalaciones	2	1	1	1	1	2	2	2	1	0	1	1	1	1	2	2	2	2	BAJO	BAJO	BAJO	Satisfactorio	Satisfactorio	BAJO
[P] Personal	2	2	2	2	2	2	2	2	1	0	2	1	1	1	2	2	2	2	MEDIO	MEDIO	BAJO	Satisfactorio	Satisfactorio	BAJO

Como podemos ver en la imagen anterior, los cálculos que hemos ido realizando nos presentan un análisis del conjunto que desemboca en un riesgo residual (que es lo importante). No se pretende en estas líneas que se crea que esta propuesta es perfecta, nada más lejos de ello, solo pretendemos que al menos creáis que es buena (recordad: *lo perfecto es enemigo de lo bueno…*). Lo que sí sabemos fehacientemente que es bueno es: que está basada en una metodología reconocida "MAGERIT" y que por tratarse de hojas de cálculo relacionadas entre sí, nos permite organizar el análisis de riesgo como un "ciclo de vida" dinámico. Esta primer "foto" que acabamos de obtener, puede no ser todo lo real que quisiera, o tal vez sí lo crea, pero dentro de un mes descubro que es mejorable. En cualquiera de estos casos, lo único que deberé hacer es modificar mis cálculos, pesos o variables para ir llevando el modelo, paso a paso, a lo que de verdad ocurre en la realidad del día a día de las redes y sistemas de TI de mi empresa, y tal cual dice MAGERIT dar respuesta a "*lo que se denomina "Proceso de Gestión de Riesgos, aconsejando que suele ser prudente una aproximación iterativa*".

Si seguimos los pasos propuestos: Acabamos de ejecutar nuestra primera iteración.

El resultado puede ser satisfactorio o no, hasta puede ser pésimo también pues ha sido nuestro primer análisis. En cualquier caso, lo que "**sí o sí**" debemos hacer es planificar acciones de mejora, sobre esto se basa el concepto de "Sistema de Gestión de la Seguridad de la Información (**SGSI**) tal cual nos propone la familia ISO/UNE 27000.

El segundo paso será ahora, evaluar diferentes posibilidades para enfrentar una primer acción de mejora. Para ello, sobre la base de las salvaguardas presentes, una buena medida es preparar tres o cuatro cursos de acción valorados, que permitirían incrementar el grado de seguridad. Otra de las grandes virtudes de lanzar una análisis de riesgo metódico, es que las acciones de mejora que implantemos serán "**medibles**", pues una vez que las

implante y las incorpore a mi sistema de cálculo, los resultados finales deberán mostrar cuantitativamente esta nueva situación.

Una vez elaborados los cursos de acción, los mismos se presentarán a formalmente a la Dirección. *¿por qué razón estamos subrayando "formalmente"*?… porque esta presentación debe realizarse con todas las formalidades que estén a nuestro alcance (convocatoria, registro, acta de reunión, presencia del comité de seguridad, de diferentes directores, etc.), una ve presentado nuestro trabajo (análisis de riesgo) y los cursos de acción propuestos: acabamos de traspasarle formalmente la responsabilidad a la dirección. Las decisiones que se adopten en esa reunión será formalmente el "riesgo residual" que quedará en nuestra empresa y con el conocimiento de todos los presentes. Por supuesto las decisiones las adoptará la dirección por lo que este riesgo queda establecido por este órgano, ante lo cual está asumiendo el riesgo del curso de acción elegido, y si dejó de lado uno que incrementaba más aún la seguridad, pues, el responsable de esas medidas que nosotros hemos propuesto formalmente y no se han adoptado es el órgano directivo que decidió no abordarlas…

Por favor, sed especialmente conscientes de la importancia de este párrafo.

Igualmente, y sólo por ahora, antes de presentarlo a la dirección, avancemos un poco más sobre ese análisis.

El título de este capítulo es "**Análisis de resiliencia de redes y sistemas**", hasta ahora hemos explicado y analizado con ejemplos una metodología de "análisis de riesgo", actividad fundamental y primaria en toda organización, pero aún no hemos relacionado estas tareas con el concepto de "resiliencia". No hay lugar a dudas que el análisis y las salvaguardas que hemos adoptado son un punto de partida que nos permite seguir avanzando iterativamente en un ciclo de mejora continua, pero el objetivo de todo este libro es redes y sistemas resilientes, así que poniendo de manifiesto ese fabuloso término de programación llamado recursividad, volvamos una vez más a las reflexiones sobre resiliencia:

Reflexión 1: Límite (umbral) elástico, plástico o de rotura.

Reflexión 2: Equilibrio entre rigidez y flexibilidad.

Reflexión 3: Calidad del material (no necesariamente precio).

Reflexión 4: Resiliente a qué.

Reflexión 5: Amortiguación (rebote).

Reflexión 6: Tiempo de respuesta óptimo.

Reflexión 7: Esfuerzo de mantenimiento.

Reflexión 8: Fisuras (o degradación).

Reflexión 9: Grado de deformación.

Reflexión 10: Presiones persistentes.

Propongo que unifiquemos un poco más estas ideas con la metodología de análisis de riesgos que acabamos de presentar.

Sigamos con nuestro ejemplo y, supongamos que en virtud de las características de nuestra empresa, hemos determinado (en esta primera iteración) que los activos críticos son los que figuran a continuación.

A su vez hagamos una catalogación preliminar sobre su posibilidad de **reposición** en el mercado o no.

Nº	Activos críticos	Valoración	Reponible
1	[files] ficheros	50.000 €	NO
2	[vr] datos vitales (vital records)	80.000 €	NO
5	[prp] desarrollo propio (in house)	35.000 €	NO
10	[dbms] sistema de gestión de bases de datos	40.000 €	SÍ
15	[backup] sistema de backup	40.000 €	SÍ
16	[host] grandes equipos	40.000 €	SÍ
23	[network] soporte de la red	10.000 €	SÍ

El concepto de reposición, como acabamos de expresar, implica que lo puedo adquirir en el mercado, haya tomado previsiones o no. Esto no quiere decir que sea ni bueno ni malo, sencillamente que deberé tratarlo de forma diferente al que NO lo encuentro en el mercado y ante una pérdida o rotura, no existe reposición en el caso de que no lo haya previsto y, he perdido el activo.

Sobre la base de estos activos que ya hemos identificado como críticos, y las reflexiones sobre las que iniciamos las ideas de Resiliencia pasemos al capítulo siguiente para continuar dándole forma a estos conceptos.

8. Matriz de Resiliencia.

Iniciaremos este capítulo, agrupando nuestras diez reflexiones en tres grupos.

- Objetivos y gestión
- Ciclo de vida
- Arquitectura de ciberdefensa

Asignaremos en los mismos las reflexiones de acuerdo al siguiente criterio.

Objetivos y gestión:

Reflexión 4: Resiliente a qué.

Reflexión 5: Amortiguación (rebote).

Reflexión 7: Esfuerzo de mantenimiento.

Ciclo de vida:

Reflexión 1: Límite (umbral) elástico, plástico o de rotura.

Reflexión 6: Tiempo de respuesta óptimo.

Reflexión 8: Fisuras (o degradación).

Reflexión 9: Grado de deformación.

Arquitectura de ciberdefensa:

Reflexión 2: Equilibrio entre rigidez y flexibilidad.

Reflexión 3: Calidad del material.

Reflexión 10: Presiones persistentes.

Como su nombre lo indica, la idea de este capítulo es ir dándole forma a una "Matriz de Resiliencia" en nuestras redes y sistemas de TI. Como toda futura estrategia, por debajo deberá desencadenar en los niveles

"Operacional" y Táctico", por lo tanto, en primer lugar debo conocer muy bien el terreno, las propias fuerzas y luego realizar la inteligencia necesaria para comprender el enemigo a enfrentar. El análisis de riesgo fue sin lugar a dudas el pilar fundamental y punto de partida, sin haber realizado el mismo sería imposible seguir avanzando, recordemos que hasta ahora no hemos hecho más que comenzar el primer ciclo de vida y a "trazo grueso" tal cual lo propone MAGERIT, este seguirá, y seguirá, y seguirá a lo largo del tiempo mejorando en cada ciclo. Tenemos nuestra foto inicial, sus activos, amenazas, impacto y salvaguardas, con esta primera visión hemos podido identificar un riesgo potencial y otro residual. Nos toca ahora seguir avanzado en este ciclo de vida, para evaluar qué capacidad de recuperación tenemos y hacia qué extremo de elasticidad la queremos llevar a lo largo del tiempo.

Para poder ir determinando la resiliencia, proponemos incorporar a cada uno de nuestros tres grupos las siguientes ideas:

Objetivos y gestión

Reflexión 4: Resiliente a qué.

Reflexión 5: Amortiguación (rebote).

- Gobierno de la Ciberseguridad.
- Gestión de riesgos.
- Gestión de incidencias.
- Plan de recuperación de desastres

Reflexión 7: Esfuerzo de mantenimiento.

- Tipo de soporte.
- precio del soporte.
- SLAs

Ciclo de vida

Reflexión 1: Límite (umbral) elástico, plástico o de rotura.

- Entorno del activo.
- Ciclos de trabajo.

- Obsolescencia.
- Redundancia.

Reflexión 6: Tiempo de respuesta óptimo.

- Gestión de copias de respaldo y recuperación.
- RTO (Restauration Time Objetive).
- RPO (Restauration Point Objetive).

Reflexión 8: Fisuras (o degradación).

- Parcheado.
- Actualizaciones.
- Formación

Reflexión 9: Grado de deformación.

- KPI - Indicadores Clave de Desempeño

Arquitectura de ciberdefensa

Reflexión 2: Equilibrio entre rigidez y flexibilidad.

- Defensa en profundidad.

Reflexión 3: Calidad del material (no necesariamente precio).

- Diseño.
- Seguridad del software.
- Componentes.

Reflexión 10: Presiones persistentes.

- Firewalls.
- Anti DDoS.
- IDSs/IPSs.

Desarrollemos cada uno de estos puntos, para poder continuar dándole forma a esta estrategia con valores medibles y cuantificables.

Grupo 1: **Objetivos y gestión**.

G1.1. Resiliente a qué:

Este será el único aspecto cuya valoración es una referencia no numérica. Se trata de describir la causa extrema que puede generar la capacidad de recuperación, identificando con máximo detalle la misma con el único objetivo de dejar expresado cuál es el mayor problema de este activo. La propuesta de causas son:

- Infección
- Corrupción
- Pérdida
- Robo
- Fallo irrecuperable (con reposición)
- Fallo irrecuperable (sin reposición)

Los aspectos que siguen serán valorados en una escala numérica de 0 a 10 y No Aplica (N/A).

G1.2. Gobierno de la Ciberseguridad:

Se trata de un procedimiento que sienta las bases de la estructura de seguridad de la organización (se verá en detalle en capítulos posteriores).

En todo este texto, cuando se trata de procedimientos, la valoración de los mismos pasa por las siguientes situaciones.

- ¿Existe?
- ¿Está completo?
- ¿Responde a una estructura documental eficiente? (búsqueda, permisos de acceso, niveles de clasificación de la información, control de integridad y de cambios, jerarquía documental)
- ¿Ha seguido un flujo de diseño, elaboración y aprobación?
- ¿Está actualizado?

- ¿Mantiene un ciclo de vida correcto?
- ¿Se encuentra debidamente implantado? (es decir es operativo, eficiente y práctico)?
- ¿Se ajusta al activo en cuestión? (desencadena en guías o manuales, contempla aspectos específicos de este activo, tiene el grado de detalle suficiente y necesario)

La escala de clasificación, como hemos mencionado, será de 0 a 10 y N/A. En el caso de los procedimientos, por supuesto siempre será subjetiva, basada en el criterio y experiencia de quien lo puntúe, por esa razón, para ser lo más preciso posible es que hemos presentado los interrogantes anteriores, sobre estas cuestiones es que se puede determinar el grado de "madurez" de un procedimiento, y el valor final, puede ser diferente a los ojos de cada auditor, pero en definitiva, si es el mismo quien completa toda la plantilla, debería ser común su criterio para todos los procedimientos.

G1.3. Gestión de riesgos:

Se trata de un procedimiento también, pero a su vez en este caso particular, se debe tener en cuenta el grado de desarrollo de todo el trabajo de gestión de riesgo que presentamos en el capítulo anterior.

G1.4. Gestión de incidencias:

También se trata de un procedimiento, pero se debe considerar también el grado de experiencia (positiva o negativa) en los casos de haber sufrido ya incidentes de seguridad. Es decir, en la valoración de este ítem, debería pesar particularmente la experiencia obtenida, si es que existió.

G1.5. Plan de recuperación de desastres:

Valoración sobre la base del nivel de desarrollo y actualización del mismo.

G1.5. Tipo de soporte:

Se refiere al soporte por parte de terceros. Es muy importante tener claro el grado de soporte que se ofrece, el nivel del mismo (1ero., 2do. y/o 3er. nivel), su capacidad técnica, el tipo de respuesta obtenida en casos anteriores, su velocidad y calidad de respuesta, el grado de satisfacción que se posee respecto al mismo, su buena voluntad en apoyar a nuestra organización (muchas veces son contratos "impuestos" que no satisfacen a las áreas operativas), su capacidad y deseo de transferir conocimiento (know how), los cursos y formación que haya impartido, su continuidad a lo largo del tiempo, su nivel de "secretismo" (Muy negativo en la calificación).

G1.6. Precio del soporte:

Este parámetro es fundamental al calificar bajo una visión de "resiliencia" pues puede impactar directamente en la decisión de los cursos de acción que adopte la dirección. Un precio óptimo (es decir máxima calificación) es cuando la relación coste/ beneficio es la esperada. Se ha puesto este parámetro, pues es muy frecuente encontrar contratos de soporte con grandes marcas o firmas o empresas cuyo renombre internacional ya de por sí implican un alto precio, pero sus resultados concretos en nuestra organización, no son el producto de esta alto precio y, seguramente, en el mercado local se encuentran otras opciones que no tienen el lastre de esa "marca internacional" y su relación coste/beneficio para nosotros es muy superior. Prestad mucha atención a este ítem, pues puede costarnos muy caro a la hora del análisis de los cursos de acción en cada ciclo de vida y en la decisión de la dirección.

G1.7. SLAs:

La valoración del soporte, muchas veces queda supeditada a los contratos que tengamos con estos proveedores, las garantías ofrecidas, tiempos de respuesta, límites, materiales y

herramientas a emplear, recursos, responsabilidades, conocimiento, etc. Un buen contrato de soporte debe contemplar con sumo detalle los acuerdos de nivel de servicio (SLA) que nos beneficien a la hora de necesitarlo.

Grupo 2: **Ciclo de vida**

G2.1. Entorno del activo:

Este ítem, se refiere a las condiciones generales de la ubicación de este activo. Si es una entorno seguro físicamente, si reúne las condiciones medioambientales, eléctricas y de refrigeración adecuadas, si esta aislado o desatendido, si es una zona peligrosa en todo sentido (terremotos, tsunamis, inundaciones, congelamiento, excesivo calor, también poblaciones marginales, etc.), si se puede llegar fácilmente al mismo, etc.

G2.2. Ciclos de trabajo:

Se debe tener en cuenta aquí el esfuerzo periódico al que está sometido, es un aspecto importante y puede llegar a ser subjetivo, pero es muy diferente el tratamiento que debemos darle a un activo que está permanentemente al límite de su uso durante largos períodos, de otro que trabaja a un porcentaje muy bajo de capacidad y de forma puntual. La probabilidad de fallo de cada uno es muy diferente, como así también su vida útil

G2.3. Obsolescencia:

Llevar un control detallado de la obsolescencia de la totalidad de los activos es vital a la hora de prever reposiciones con el tiempo suficiente como para evitar sorpresas. un activo que se aproxima a estas fechas no puede puntuarse igual que uno que acaba de iniciar su período de funcionamiento.

G2.4. Redundancia:

Cuando un activo crítico debe mantenerse en alta disponibilidad, el diseño de su redundancia es uno de los factores clave. En este tipo de casos, deberá penalizarse seriamente a los que no tengan implantadas medidas robustas de redundancia.

G2.5. Gestión de copias de respaldo y recuperación:

nuevamente estamos frente a un procedimiento y desde el punto de vista de la Resiliencia, este tal vez sea uno de los más importantes. En particular para su puntuación, es muy importante verificar las pruebas periódicas de recuperación, el control y supervisión de copias, la actualización de lo que debe ser resguardado, las plataformas que se emplean, y el conocimiento del personal que hace uso de las mismas.

G2.6. RTO (Restauration Time Objetive):

Tiempo de restauración del backup o ventana de tiempo en la que el backup ha de ser recuperado. Es decir, ¿en cuánto tiempo debe estar nuevamente en producción? Este punto suele ser motivado por un análisis de riesgo previo, pues no necesariamente deben tener todos los dispositivos la misma prioridad o impacto para la organización a la hora de recuperar su funcionamiento normal. En este ítem, estamos hablando de un activo crítico, por lo que se debe ser estricto en su calificación, el tiempo definido para este activo debe contar con un estudio serio y que refleje tanto la necesidad del negocio en su recuperación, como la realidad o factibilidad de cumplirlo. En la puntuación de este ítem, se deberá hacer todo el esfuerzo posible para analizar si es cierto que estamos en capacidad de cumplirlo

G2.7. RPO (Restauration Point Objetive):

Punto a partir del cual ha de ser posible restaurar un backup, un software o un fichero expresado en horas, días o semanas según proceda. Es decir, ¿cuántos datos puedo llegar a perder?, ¿Es necesario actualizar cada hora, cada día, cada semana, cada

mes? Sobre este punto aplican las consideraciones del punto anterior y a su vez se suma el carácter "dinámico o estático" que tenga cada plataforma o dispositivo, pues existen algunos de ellos cuyas configuraciones no suelen ser modificadas por meses o años (Ej: grandes Switchs, Proxies), y por el contrario dispositivos que se modifican varias veces al día (Ej: LDAP; TACACS, Servidores de Logs). Al igual que el punto anterior, su valoración debe ser analizada en detalle y aplican los conceptos del párrafo anterior.

G2.8. Parcheado:

La política de parcheado, ya se ha visto con los actuales tipos de malware al estilo "Ransomware", que es una actividad imprescindible. En esta puntuación, se debe tener en cuenta el cumplimiento y nivel de actualización del mismo, como así también las plataformas de gestión de parcheado (que incluyan pruebas de maqueta y parcheados masivos).

G2.9. Actualizaciones:

Es muy similar al punto anterior, y en su puntuación se prestará especial atención al nivel de cumplimiento con lo que indique el fabricante o proveedor.

G2.10. Formación:

En este ítem, se debe considerar específicamente la formación del personal en relación directa con el activo que se está puntuando. Esta formación debe cubrir tanto aspectos de seguridad, como de recuperación de desastres, de operación del activo, de respaldo y recuperación, de conocimiento de la documentación que impacta sobre el activo, de procedimientos de seguridad, de escalado y proceder ante incidentes, etc. Deberá penalizarse estrictamente los fallos de formación, pues es el factor humano la pieza clave de la resiliencia de nuestras redes y sistemas.

G2.11. KPI - Indicadores Clave de Desempeño:

Este ítem debería relacionarse en forma directa con lo que establece la norma ISO/UNE 27004. Lo importante aquí es que como parte de este ciclo de vida que da nombre al grupo que estamos desarrollando, se ponga de manifiesto que estas KPI, métricas o indicadores han sido definidos, son útiles paga la gestión de la seguridad, se miden adecuadamente, y son o serán motivo del análisis de mejora de cada ciclo, ofreciendo herramientas de juicio válidas para adoptar decisiones clave en el ciclo de vida.

Grupo 3: **Arquitecura de Ciberdefensa**

G3.1. Defensa en profundidad:

Se trata aquí de tener organizada la defensa por capas, dándole profundidad a la arquitectura de la red, colocando los activos menos críticos en la periferia comúnmente denominada DMZ (Zona Desmilitarizada), luego al menos una segunda zona también frecuentemente nombrada como MZ (Zona Militarizada) y luego los activos más críticos en un Core o Línea a no ceder (puede verse en detalle en el libro "**Seguridad en Redes**").

G3.2. Diseño:

El diseño de una arquitectura de red debe contar con un área de lo organización específico para ello que será responsable de la asignación de direcciones, zonas, nombres y funciones, preparará la arquitectura inicial e irá velando para su expansión de forma flexible y segura. Una red bien diseñada debe permitir su expansión de forma sencilla y siempre contemplando las zonas o áreas de seguridad para cada activo. Otro parámetro fundamental de diseño es la segmentación de redes de gestión y servicio totalmente aisladas entre sí.

G3.3. Seguridad del software:

En este ítem nos estamos refiriendo al "desarrollo seguro de software", actividad que debe ser tenida en cuenta, tanto en los desarrollos propios como subcontratados. Hay mucha bibliografía sobre el tema y hasta hay software que permite valorar, monitorizar y supervisar el ciclo de vida del mismo para poder determinar si se degrada o mejora, a medida que se incorporan nuevos módulos o funcionalidades.

G3.4. Componentes:

Muchos activos, aparte de las dependencias que identificamos en el análisis de riesgo, están conformados por diferentes componentes. Un caso típico puede ser un robot de backup, que se conforma por una parte mecánica, otra de discos, un software y sus sistemas de red, eléctricos y medioambientales. Sin llegar a tanta complejidad en muchos casos mas sencillos, también es posible valorar la existencia de algún componente que tire abajo el funcionamiento global del activo. Se debe prestar especial atención en identificar estos casos, pues es bien conocido que "una cadena se corta por el eslabón más débil".

G3.5. Firewalls:

Este es un punto fundamental a considerar, y en especial porque no sólo nos interesa que existan o no, sino que debemos ser rigurosos aquí en cuanto a su diseño, gestión, actualización de reglas, gestión de Logs, procedimientos, políticas, reglas ajustadas o no, sistemas de ticketing en todas sus acciones, monitorización y supervisión de los mismos, etc.

G3.6. AntiDDoS:

Esta funcionalidad o servicio externalizado, nos da la garantía para no quedarnos fuera de servicio ante este tipo de ataques masivos. Suele ser una funcionalidad cara de precio si se subcontrata o si adquieren las herramientas comerciales o appliances del mercado, pero existen también soluciones creativas y novedosas combinando IDSs con routers y sistemas de derivación de tráfico por medio de protocolos dinámicos. Se debería valorar especialmente para activos expuestos a redes externas.

G3.7. IDSs/IPSs:

Este ítem también es muy importante en una arquitectura de ciberdefensa y tal vez sea una de las claves que demuestran la capacidad de detección temprana y análisis de lo que está sucediendo, para poder tener la libertad de acción en la forma de recuperar mis redes y sistemas ante un incidente. Si en los primeros pasos aún no están contemplados, es una de los mejores desafíos a proponer para ir incrementando el nivel de resiliencia a lo largo de cada ciclo.

Acabamos de describir cada uno de estos ítems, sobre los que iremos calificando estos agrupamientos presentados, sobre las reflexiones de resiliencia. Para organizarnos y poder explotar bien estos conceptos, podemos desarrollar una sencilla plantilla de cálculo que nos permita tener una foto inicial de cómo veo reflejado el conjunto a fecha de hoy, y a su vez comenzar a estudiarlos a lo largo del tiempo, identificar acciones y pasos que pueda seguir para ver evolucionar a mejor el conjunto y a su vez cada uno de ellos. Para seguir profundizando en el tema, pongamos un ejemplo de ello.

				Objetivos y gestión								Ciclo de vida										Arquitectura de ciberdefensa					
Nº	Activos críticos	Valoración	Repo-nible	Resiliente a qué	Gobierno de la Ciberse-guridad	Gestión de riesgos	Gestión de inci-dencias	Plan de recupera-ción de desastres	Tipo de soporte	precio del soporte	SLAs	Entorno del activo	Ciclos de trabajo	Obsoles-cencia	Redun-dancia	RTO	RPO	Par-cheado	actuali-zaciones	for-mación	KPI	Defensa en profun-didad.	Seguridad del software	Compo-nentes	FWs	Anti DDoS	IDSs / IPSs
1	[files] ficheros	50.000 €	NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
2	[vr] datos vitales (vital records)		NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
5	[prp] desarrollo propio (in house)	35.000 €	NO	Infección, Corrupción, Robo	6	6	5	4	8	8	4	9	7	N/A	7	1	1	N/A	7	4	2	9	8	N/A	9	3	2
10	[dbms] sistema de gestión de bases de datos	40.000 €	SÍ	Fallo irrecuperable:CR	7	6	5	4	5	7	4	9	5	2	9	N/A	N/A	9	9	4	2	9	8	9	9	3	2
15	[backup] sistema de backup	40.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	4	5	7	4	9	5	2	7	N/A	N/A	9	9	4	2	9	8	9	9	N/A	2
16	[host] grandes equipos	40.000 €	SÍ	Fallo irrecuperable:SR	8	6	7	7	8	7	8	5	7	8	7	1	1	9	9	4	2	9	N/A	9	9	3	2
23	[network] soporte de la red	10.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	7	8	7	8	5	7	8	N/A	N/A	N/A	9	9	4	2	9	N/A	9	9	N/A	2
	Suma Total:	215.000 €			53	42	41	34	44	46	36	55	41	20	48	4	4	36	43	28	14	63	24	54	63	15	14
	Promedios:				7,57	6,00	5,86	4,86	6,29	6,57	5,14	7,86	5,86	5,00	8,00	1,00	1,00	9,00	8,60	4,00	2,00	9,00	8,00	9,00	9,00	3,00	2,00

La plantilla presentada aquí arriba es solo un ejemplo, con valores que hemos ido asignando según nuestro criterio, para poder hacer una análisis de una situación hipotética que nos permita seguir adelante con esta propuesta de trabajo.

Como podemos apreciar, hemos puesto diferentes colores a los grupos, valorado cada ítem respecto a nuestros activos críticos, y la misma plantilla nos pone en **rojo** cualquier valor inferior a "4" para resaltar nuestra atención sobre los mismos.

Esta plantilla es solo una propuesta de un método de trabajo, en el que cada uno puede ajustarlo para su mejor empleo, tanto en los parámetros que desencadenaron de las reflexiones, en las escalas de puntuación o en su

forma y presentación. El objetivo fundamental de esta propuesta es avanzar en nuestra "Matriz de Resiliencia" que como veremos a continuación sigue con la lógica de ciclo de vida de las ciberdefensa para que, tal cual lo propone la familia ISO/UNE 27000, paso a paso generemos un ciclo de mejora continua de la seguridad.

Hagamos un análisis más de la plantilla recientemente presentada.

				Objetivos y gestión								Ciclo de vida									Arquitectura de ciberdefensa					
Nº	Activos críticos	Valoración	Repo-nible	Resiliente a qué	Gobierno de la Ciberse-guridad	Gestión de riesgos	Gestión de inci-dencias	Plan de recupera-ción de desastres	Tipo de soporte	precio del soporte	SLAs	Entorno del activo	Ciclos de trabajo	Obsole s-cencia	Redun-dancia	RTO	RPO	Par-cheado	actuali-zaciones	for-mación	KPI	Defensa en profun-didad	Seguridad del software	Compo-nentes	FWs	Anti DDos	IDSs / IPSs
1	[files] ficheros	50.000 €	NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
2	[vr] datos vitales (vital records)		NO	Corrupción, Pérdida, Robo	8	6	5	4	5	5	4	9	5	N/A	9	1	1	N/A	N/A	4	2	9	N/A	9	9	3	2
5	[prp] desarrollo propio (in house)	35.000 €	NO	Infección, Corrupción, Robo	6	6	5	4	8	8	4	9	7	N/A	7	1	1	N/A	7	4	2	9	8	N/A	9	3	2
10	[dbms] sistema de gestión de bases de datos	40.000 €	SÍ	Fallo irrecuperable:CR	7	6	5	4	5	7	4	9	5	2	9	N/A	N/A	9	9	4	2	9	8	9	9	3	2
15	[backup] sistema de backup	40.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	4	5	7	4	9	5	2	7	N/A	N/A	9	9	4	2	9	8	9	9	N/A	2
16	[host] grandes equipos	40.000 €	SÍ	Fallo irrecuperable:SR	8	6	7	7	8	7	8	5	7	8	7	1	1	9	9	4	2	9	N/A	9	9	3	2
23	[network] soporte de la red	10.000 €	SÍ	Fallo irrecuperable:CR	8	6	7	7	8	7	8	5	7	8	N/A	N/A	N/A	9	9	4	2	9	N/A	9	9	N/A	2
	Suma Total:	215.000 €			53	42	41	34	44	46	36	55	41	20	48	4	4	36	43	28	14	63	24	54	63	15	14
	Promedios:				7,57	6,00	5,86	4,86	6,29	6,57	5,14	7,86	5,86	5,00	8,00	1,00	1,00	9,00	8,60	4,00	2,00	9,00	8,00	9,00	9,00	3,00	2,00

Como se aprecia en la imagen anterior, estamos presentando nuevamente con colores los aspectos que según nuestro criterio deberían ser tratados con más detalle. Se ha remarcado en **"rojo"** los aspectos que mas impactan en nuestra estrategia de resiliencia, en color "naranja" los que le siguen y en **"azul"** nuestros puntos fuertes.

Profundicemos en cada uno de ellos.

(1) y **(2)** nos indican que evidentemente aún no hemos puesto ningún tipo de atención sobre los cálculos de **RTO**, ni **RPO** justamente en estos activos que son críticos. Justamente estos parámetros no aplican (N/A) en los sistemas de gestión, de backup y en los soportes de red, pues se tratan de plataformas o componentes que mantienen su funcionamiento a lo largo del tiempo y que justamente son "reponibles", es decir que ante una anomalía, se reparan físicamente, se les carga su software original o se adquieren nuevamente. Sin embargo sí impactan en "datos" y en la configuración final de nuestros grandes equipos.

Una valoración de "1" nos esta imponiendo que adoptemos algún tipo de acción pues evidentemente nuestra situación en cuanto a "Resiliencia" en estos ítems es pésima.

(3) Nos pone de manifiesto que aún no tenemos definidos **KPIs**, estos indicadores clave de rendimiento, en definitiva son métricas que al ser consideradas y valoradas periódicamente nos

presentan una clara visión del ciclo de vida, y si las sabemos definir adecuadamente, nos reflejarán la realidad de los puntos críticos de nuestra organización de la Ciberdefensa. Estos KPIs cuando maduran a lo largo del tiempo son los que nos alertan de cualquier desvió o nos permiten adoptar medidas o acciones productivas y preventivas para mantener el estado deseado y que no se degraden nuestros umbrales alcanzados.

(4) Si bien, mejora un punto su calificación, nos pone de manifiesto que el trabajo con **IDSs/IPSs,** si bien es probable que ya se haya iniciado, evidentemente está inmaduro o aún no lo estamos haciendo bien.

(5) Nos indica un hecho puntual muy importante, en este caso, nuestros sistemas de gestión de backup y de bases de datos, se encuentran próximos a su fecha de obsolescencia. Hemos intentado remarcar este hecho, pues llevar un correcto control de obsolescencia es una de las tareas más importantes de un "diseño Resiliente". La realidad nos ha demostrado que una de las peores situaciones que se pueden vivir ante una anomalía o incidencia, es que cuando necesitamos imperiosamente recuperar un elemento, nos desayunamos (recién ahí) que esta obsoleto, fuera de soporte o ya no encontramos ese modelo en el mercado. Este tipo de situaciones las hemos vivido varias veces y su efecto ronda en lo devastador.

Un muy buen control de obsolescencia nos evita este tipo de dolores de cabeza, y por supuesto nos garantiza en muchos aspectos el nivel de resiliencia que buscamos.

(6) Si bien apreciamos una puntuación mejor, nos demuestra que hemos tomado algunas acciones en medidas AntiDDoS, pero evidentemente debemos hacerlo mejor.

(7) Este es otro valor que intencionalmente quisimos poner de manifiesto. Como podemos aprecia, no se trata de un tema de puntuación, sino de un aspecto más subjetivo. Quien rellenó estos valores, es consciente que en algunos, o quizás todos, sus grandes equipos tiene problemas ante un fallo irrecuperable pues NO posee reposición. Esta e otra situación bastante frecuente y por esa razón quisimos remarcarla como un hecho a tener

especialmente en cuenta desde el punto de vista de la resiliencia. Es más frecuente de lo deseado, que se descabalguen modelos de hardware o software. Este hecho no presenta inconvenientes cuando las versiones futuras presentan compatibilidades con las descabalgadas, pero sí lo es (y grave) cuando NO presentan compatibilidad. Es decir, nos encontramos en una situación en la cuál sabemos y somos conscientes, en este caso concreto que tenemos uno o varios grandes equipos que si sufren un fallo irrecuperable, NO podemos reponerlos pues los modelos que puedo adquirir ahora NO son compatibles con otros componentes (tarjetas, periféricos, conexiones físicas, etc.) o con el software que se ejecuta en el mismo (sistema operativo, aplicaciones, desarrollos, lenguajes, etc.).

Si prestamos atención, el evaluar "Resilientes a qué", nos obliga a considerar este tipo de cuestiones, tomar contacto con nuestros proveedores, garantizar compatibilidades, buscar opciones en el mercado, evaluar competencias de producto, etc. Este trabajo, nos permitirá asegurar que ante un fallo en este tipo de activos críticos, tenemos una alternativa y no nos encontremos, llegado el caso, en un callejón sin salida.

(8) Como se pone de manifiesto por su color **"naranja"** ya estamos tratando ítems o problemas de menor envergadura desde el enfoque resiliente de nuestras redes y sistemas de TI. En este caso la valoración es clara y representativa, hemos trabajado algo en temas de formación en ciberseguridad, pero somos conscientes que debemos profundizar más.

(9) Esta es otra valoración que hemos querido poner de manifiesto. Si bien vemos que no es tan crítica como los valores rojos, nos encontramos ante una situación en la cual justamente debería llamarnos la atención, pues los valores más bajos ("4") se encuentran en los activos más importantes de mi organización, este **DRP** (Disaster Recovery Plan), se encuentra bien ("7") en mi equipamiento y en la red, pero justamente NO está bien en los activos que guardan relación con los "datos" que presentamos desde el principio como lo más representativo, y más aún para una ejemplo de empresa que vive de ello.

(10) Este punto, ofrece conceptos similares al anterior, lo más flojo son los "datos" y justamente sobre ellos es que los niveles de SLAs que tengo firmados, no son los mejores.

(11) Estamos pasando ahora a los aspectos positivos, o fortalezas que presenta mi análisis. En este caso puntual, se pone de manifiesto que he alcanzado un nivel casi óptimo de **parcheado**, con lo que me indica que hay una baja posibilidad de sufrir ataques de día cero.

(12) Haber valorado bien este ítem, nos indica que tenemos una arquitectura robusta en capas de defensa, zonas de seguridad y bien segmentada.

(13) Las decisiones sobre adquisición de **componentes** en estos activos críticos, evidentemente ha sido acertada. Es muy buena práctica evidenciar este tipo de hallazgos, pues en futuras adquisiciones o reposiciones, se es consciente que si bajo este nivel o escatimo gastos en estos parámetros sobre estos activos críticos, se produciría una degradación directa de este umbral alcanzado. Podría hacerlo sobre otro tipo de elementos, pero NO sobre estos que ya identifiqué como críticos.

(14) Se ha realizado un trabajo metódico en el proceso de gestión de **FWs**, lo cual es muy coherente también con el valor del punto (12) pues son dos aspectos que van muy de la mano.

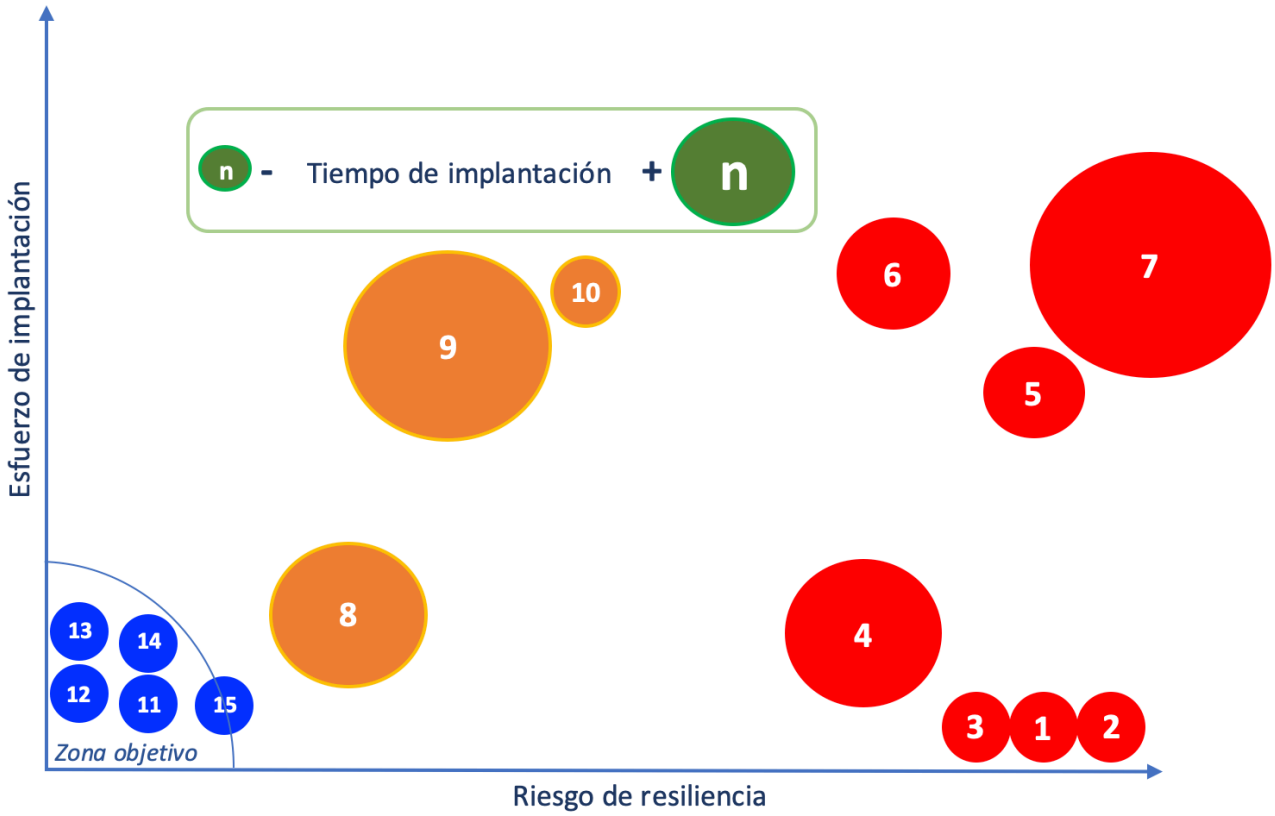
(15) En nuestra empresa se está haciendo bastante hincapié en las metodologías de "desarrollo seguro de software", lo que desde el punto de vista de resiliencia es casi una garantía de éxito.

Como hemos podido apreciar, en el ejemplo propuesto por la matriz de análisis, se han tratado de destacar aspectos importantes de esta metodología de trabajo, como para que le puedan ser de utilidad y ejemplo al lector, para llevarlos a la práctica en su propia organización. Repetimos, que se trata de una propuesta y metodología de trabajo que debe ser tomada en cuenta como una herramienta al servicio de la Resiliencia, la cual es personalizable y ajustable a cada red y sistema en particular, hasta que el administrador de la misma se sienta a gusto con su diseño, evolución y le

permita a, su vez, adoptarla como un "ciclo de vida" de la resiliencia de su organización.

9. Estrategias Resilientes en Redes y Sistemas.

Para seguir avanzando ahora hacia nuestra estrategia de resiliencia, proponemos a continuación que se sigan haciendo valoraciones sobre los resultados obtenidos, esta vez nos centraremos en esfuerzos, tiempos y riesgos. Una vez más según nuestro criterio hemos asignado valores a estos conceptos, para que podemos desarrollar el tema de forma eminentemente práctica. Nuevamente reiteramos que este tipo de asignaciones son según nuestra propia forma de ver el tema y con la única intención de darle una forma entendible y clara, quedando como siempre a criterio del lector aplicar su propio punto de vista al respecto y con toda la libertad de compartirlo, o no. Nuestra propuesta se lleva a cabo teniendo en cuenta la imagen que se presenta a continuación.



Lo primero que se pone de manifiesto en la imagen anterior, es la zona objetivo, en la cual como es de esperar se encuentran los aspectos positivos de nuestra evaluación, prestad atención que el ítem **(15)** se encuentra en la

frontera de la misma, pues su valoración global fue de "**8**" puntos (la más baja de la zona **azul**).

Como indica la misma imagen, el tamaño de cada círculo representa el tiempo de implantación, los ejes "x" el riesgo desde el punto de vista de la resiliencia y el eje "y" el esfuerzo de implantación (medido en recursos humanos y materiales).

Es evidente que cuanto más a la derecha del cuadro nos encontramos, mayor es el riesgo que hemos asignado a esos ítems, en este caso se tratarían de **(7)**, **(2)**, **(1)**, **(5)** y **(3)** en segundo orden podemos situar a **(4)** y **(6)**, y luego nos quedarían los tres color naranja, cuya calificación estaría por arriba de los "4" puntos y hemos determinado un grado menor de criticidad, ellos son **(8)**, **(9)** y **(10)**.

Si prestamos atención al eje de las "Y" veremos que hay ítems que nos requerirán mayor esfuerzo de implantación, en este caso son **(7)**, **(6)**, **(10)**, **(9)** y **(5)**.

Por último, nos interesa analizar su tamaño en el cuadro que nos pone de manifiesto que los ítems **(7)**, y **(9)** nos requerirán más tiempo de implantación y en segundo orden estarían el **(8)** y el **(4)**.

Hemos logrado identificar en un cuadro de dos dimensiones, tres tipos diferentes de magnitudes que nos permitirán seguir adelante con nuestra "estrategia de resiliencia". Para poder ser aún mas detallistas, proponemos ponerles nombres que sean representativos para nosotros y comenzar a evaluar un plan de acción para abordarlas. En nuestro caso, nuevamente lo haremos a través de una plantilla, que se presenta a continuación:

Valor	Actividad	AÑO 1												AÑO 2										Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																							500 €	1	1º Sem	
(2)	Determinación de RPO																							500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas			Ajustes/Medición																	700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs	Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta													1.500 €	3		
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																			4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS	Análisis/presupuestos			Pruebas		Implementación																	5.000 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)				2da. Compra/despliegue			E. producción (2da.compra)				Pruebas finales/Mejoras			9.000 €	1	1º año	2º año
(8)	Formación				Plan formación			Fase 1			Med. Resultados			Fase 2			Med. Resultados			Fase 3		Med. Resultados		Eval fimal/mejoras	1.500 €	5	2ºSem	2º año
(9)	DRP				Análisis			Fase 1			Pruebas			Fase 2			Pruebas			Fase 3		Pruebas		Aprobación/Mejoras	4.500 €	5	2ºSem	2º año
(10)	SLAs	<-- **1 mes** --> (desplazable según presupuesto y costes)																						4.500 €	4	Ajustable	
																								31.700 €		19.700 €	7.500 €
																										4.500 € (ajustable)	

Estudiemos la plantilla de la imagen anterior.

Estamos presentando un análisis temporal dos años de duración, dividido en cuatro semestres, y a su vez la plantilla nos muestra también su posible evolución mes a mes.

Hemos centrado la atención en los diez ítems que anteriormente identificamos con mayo riesgo, le hemos puesto los siguiente nombres:

(1) Determinación de RTO

(2) Determinación de RPO

(3) Determinación de KPIs

(4) Mejoras en IDSs/IPSs

(5) Obsolescencia BBDD y Backups

(6) Mejoras en AntiDDoS

(7) Reposición de grandes equipos

(8) Formación

(9) DRP

(10) SLAs

Para nosotros ahora, cada uno de esos ítems son "**Actividades**" que debemos organizar cómo deseamos abordarlas. Se puede apreciar, en cada línea de estas la propuesta que según nuestro criterio, sería la adecuada en su tratamiento. Es importante tener en cuenta en esta planificación temporal, que su "duración" ha sido considerada sobre la base del tamaño de cada uno de los círculos del cuadro anterior, es decir, la **(7)**, **(8)** y **(9)** se ve claramente que duran 2 años, le sigue la **(4)** que dura solo un año, y los círculos más pequeños solo algunos meses.

Otro hecho que hemos reflejado en la plantilla, es que las actividades que mayor riesgo tienen **(7)**, **(1)** y **(2)** se prevén lanzar de inmediato, luego las actividades **(3)**, **(5)** y **(6)**, si bien también se planifican desde el primer mes, su implantación real, podemos ver que es a partir del mes 4. A partir de allí es cuando se comienzan a abordar el resto. Cabe mencionar aquí que los acuerdos de nivel de servicio (SLAs:**(10)**) nos hemos permitido "ajustar" su implantación a cuando mejor nos cuadre.

A la derecha de nuestra nueva plantilla podemos ver una zona coloreada en **"gris"** que es la parte en que, en la primera columna, realizamos una primera aproximación de costes. Nuevamente, aquí lo hacemos basándonos en el cuadro y teniendo en cuenta el eje "Y" del mismo, pues cuanto más "alta" se encuentre la actividad, mayor esfuerzo de implantación requerirá (material y/o humano). Podemos notar aquí que las actividades **(1)**, **(2)**, **(·3)** que son las que se encuentran el la parte inferior

del cuadro, son las que económicamente menor coste tienen y, en este ejemplo en concreto, guardan relación no con gasto económico, sino con horas hombre de trabajo. En el extremo opuesto vemos la actividad **(7)** que es la más onerosa, seguidas de la **(6)**, **(10)**, **(9)** y **(5)**.

En la columna **"gris"** que sigue, vemos que nuevamente evaluamos la "**prioridad**". Como cabe esperar, este valor guarda relación con el riesgo que ya hemos puesto a cada una de ellas, pero también considerando su temporalidad. Esta nueva prioridad es uno de los valores que nos permitirá ir dándole forma a los diferentes cursos de acción que propondremos finalmente a la Dirección.

Por último se presentan las dos columnas **"grises"** que tienen por objetivo, distribuir estos costes estimados a lo largo de los dos años previstos.

Todos estos cálculos económicos, como podemos ver tienen sus correspondientes totales en las filas inferiores.

El resultado final al que deberíamos apuntar es poder darle forma sólida y medible a diferentes cursos de acción, para poder presentarlos con solvencia ante la dirección, y esta que es la que conoce su capacidad de inversión y a su vez si hemos sido capaces de obtener su compromiso e involucramiento en la Ciberdefensa de nuestra empresa (tal cual lo establece la familia IS/UNE 27000), será la que pueda establecer la relación adecuada de coste/beneficio, siendo consciente de la capacidad de gasto e inversión de toda la organización como un conjunto.

A continuación, presentamos, nuevamente a título de ejemplo, cómo podríamos definir estos cursos de acción.

a. Curso de acción "de máxima".

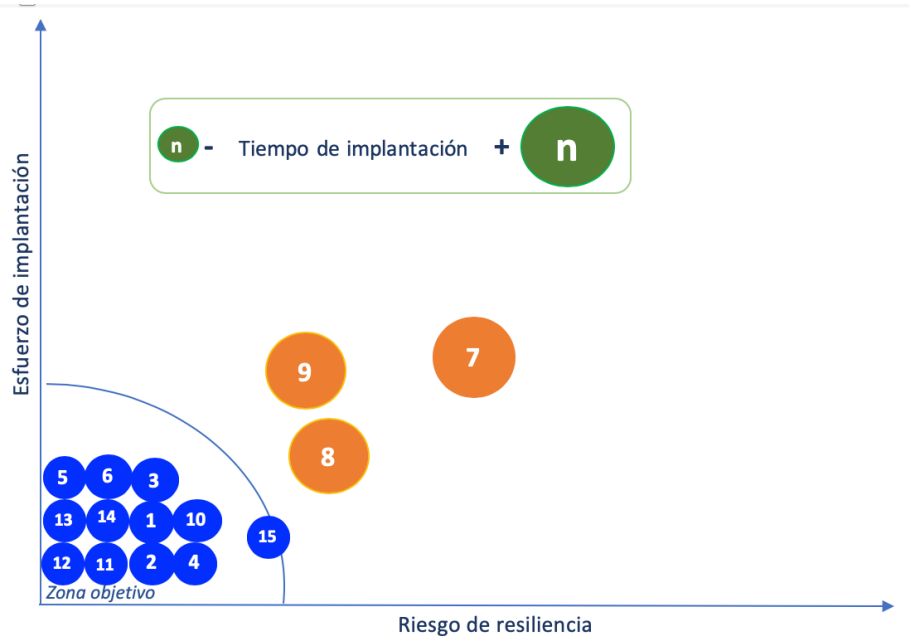
Este curso de acción, propone abordar el 100% de las acciones propuestas en los tiempos calculados, dando cumplimiento detallado a toda la planificación presentada en la plantilla inicial. El coste que implica para la empresa son **31.700 €** a pagar de la siguiente forma:

19.700 € + 4.500 € = 24.200 € el primer año

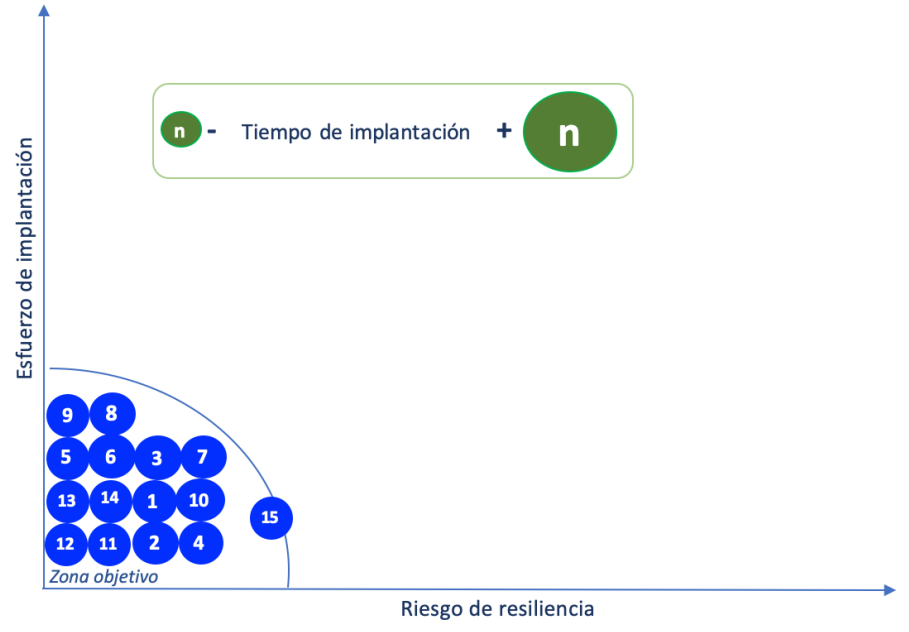
7.500 € el segundo año

El resultado final de este curso de acción se verá reflejado de la siguiente forma.

A finales del primer año.



A finales del segundo año.



b. Curso de acción "intermedio".

Este curso de acción, propone abordar el **85%** de las acciones propuestas en los tiempos calculados, el coste que implica para la empresa son **24.200 €** a pagar de la siguiente forma:

17.700 € el primer año

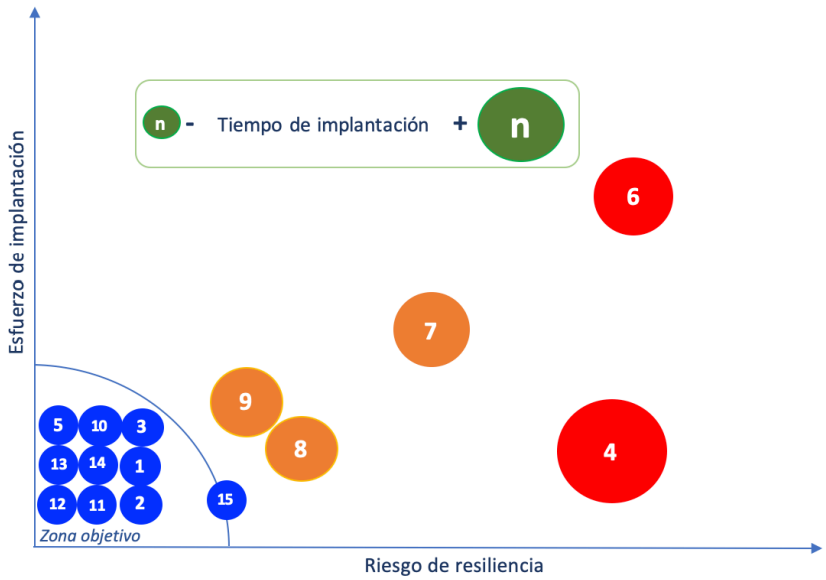
6.500 € el segundo año

En este curso de acción intermedio, se modifica la planificación y asignación de actividades de la siguiente forma:

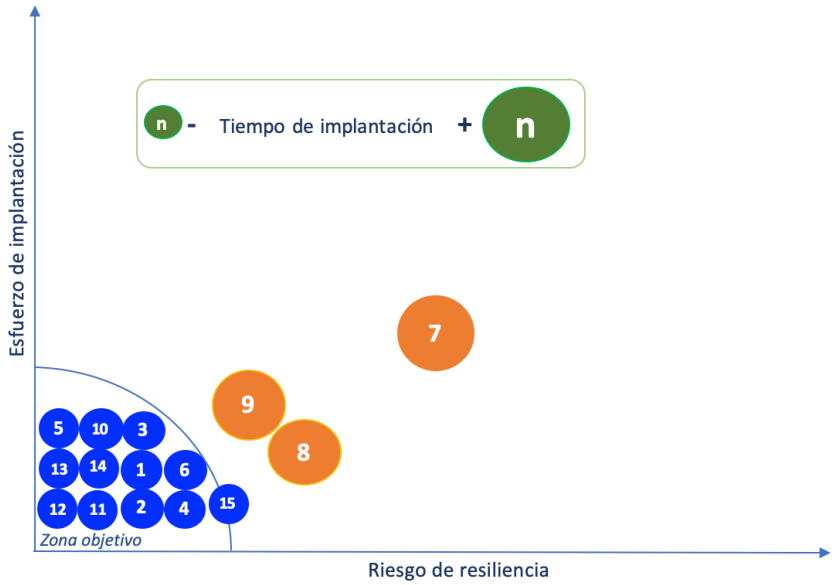
Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas			Ajustes/Medición																			700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño		nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta				1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS													Análisis/presupuestos			Pruebas		Implementación							5.000 €	3		2º año
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)				NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1			Pruebas			NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año	
																										24.200 €		17.700 €	6.500 €

El resultado final de este curso de acción se verá reflejado de la siguiente forma

A finales del primer año.



A finales del segundo año.



c. Curso de acción "de mínima".

Este curso de acción, propone abordar el **60%** de las acciones propuestas en los tiempos calculados, el coste que implica para la empresa son **16.700 €** a pagar de la siguiente forma:

9.200 € el primer año

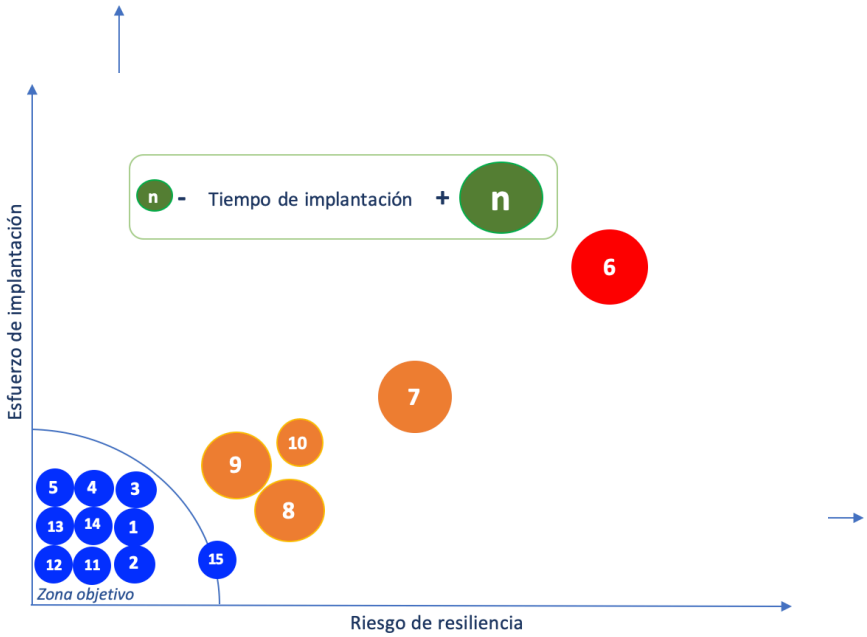
7.500 € el segundo año

En este curso de acción de mínima, se modifica la planificación y asignación de actividades de la siguiente forma:

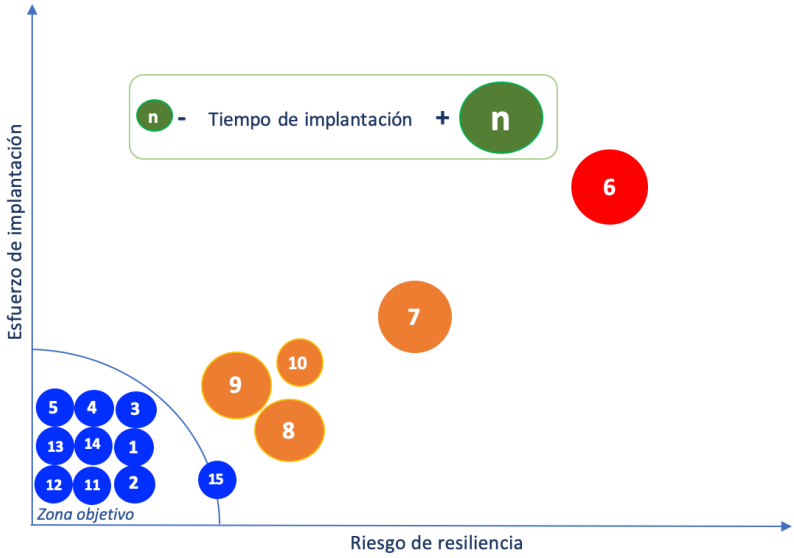
Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas		Ajustes/Medición																				700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño		nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta				1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups													Análisis/presupuestos		Implementación										4.000 €	2		2º año
(6)	Mejoras en AntiDDoS																									0 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración		1ra. Compra/despliegue				Entrada producción (1ra.compra)			NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1			Pruebas			NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs													Firma de nuevos contratos (con mínimos SLAs)												2.000 €	4		2º año
																										16.700 €		9.200 €	7.500 €

El resultado final de este curso de acción se verá reflejado de la siguiente forma

A finales del primer año.



A finales del segundo año.



El haber realizado un trabajo con tanto nivel de cálculo y granularidad, nos permite desde presentar el nivel de detalle máximo a las áreas que lo necesiten, hasta poder crear presentaciones ejecutivas de alto nivel que con solo una imagen quede reflejado todo el proyecto para un alto directivo.

Todo este trabajo, nos permite presentar ante la dirección un informe sólido, que demuestra que tiene una metodología completa de análisis por detrás y que le hemos dedicado el tiempo suficiente como para ofrecer soluciones concretas, y sobre todo, cuantifícales y medibles.

Cuando se hace un trabajo de este tipo, se crea un doble vínculo, el de la dirección de asignarnos una partida suficiente para cumplir nuestros compromisos y la obligación por nuestra parte de llevarlo a cabo de la forma en que lo expusimos, pues los resultados finales de cada etapa pueden (y deben) poder ser medidos y expuestos como "hitos" de cumplimiento.

Por último presentamos una imagen final donde se aprecian las diferentes opciones que podrían ofrecerse en una sola imagen a la alta dirección para que adopte la mejor decisión que crea pertinente, por supuesto que nuestra labor será demostrar que lo óptimo es el primer curso de acción y poner todo nuestro esfuerzo para lograr el curso de acción de máxima.

a. Curso de acción de máxima

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas		Ajustes/Medición																				700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs	Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta															1.500 €	3		
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS	Análisis/presupuestos			Pruebas			Implementación																		5.000 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos						Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)			2da. Compra/despliegue			E. producción (2da.compra)				Pruebas finales/Mejoras			9.000 €	1	1º año	2º año
(8)	Formación				Plan formación			Fase 1			Med. Resultados			Fase 2			Med. Resultados			Fase 3			Med. Resultados		Eval fimal/mejoras	1.500 €	5	2ºSem	2º año
(9)	DRP				Análisis			Fase 1			Pruebas			Fase 2			Pruebas			Fase 3			Pruebas		Aprobación/Mejoras	4.500 €	5	2ºSem	2º año
(10)	SLAs	<-- 1 mes --> (desplazable según presupuesto y costes)																								4.500 €	4	Ajustable	
																										31.700 €		19.700 €	7.500 €
																												4.500 € (ajustable)	

Coste: 31.700 €

a pagar:

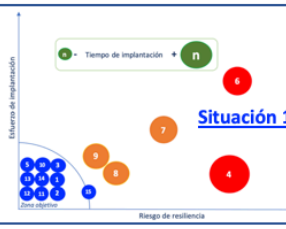
24.200 € el primer año

7.500 € el segundo año

se aborda el **100%** de las acciones

b. Curso de acción intermedio

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas		Ajustes/Medición																				700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta		1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS													Análisis/presupuestos			Pruebas			Implementación						5.000 €	3		2º año
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)				NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1			Pruebas			NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año	
																										24.200 €		17.700 €	6.50



Coste: 24.200 €

a pagar:

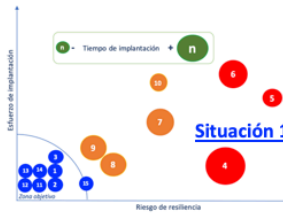
17.700 € el primer año

6.500 € el segundo año

se aborda el **85%** de las acciones

c. Curso de acción de mínima

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas		Ajustes/Medición																				700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño			nuevas configuraciones			ajuste reglas			Pruebas funcionam. Planta		1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups													Análisis/presupuestos			Implementación									4.000 €	2		2º año
(6)	Mejoras en AntiDDoS																									0 €	3		
(7)	Reposición de grandes equipos	Análisis/presupuestos			Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)				NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1			Pruebas			NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs													Firma de nuevos contratos (con mínimos SLAs)												2.000 €	4		2º año
																										16.700 €		9.200 €	7.50



Coste 16.700 €

a pagar:

9.200 € el primer año

7.500 € el segundo año

se aborda el **60%** de las acciones

La decisión que adopte la dirección de mi empresa, será la "**Estrategia de Resiliencia**" que adoptaremos, en nuestro ejemplo, para los próximos dos años.

10. Ciclo de Vida.

Para seguir manteniendo como referencia de este libro los estándares internacionales, este capítulo lo basaremos en la familia ISO/UNE 27000.

Comenzaremos desarrollando algunos conceptos de la primera versión del estándar ISO/UNE 27001, es decir la del año 2005, luego continuaremos por la última versión del año 2017.

La primera versión de este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del **SGSI** (Sistema de Gestión de la Seguridad de la Información), la adopción del SGSI debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

Este estándar internacional adopta también el modelo "Plan-Do-Check-Act" (**PDCA**), el cual es aplicado a toda la estructura de procesos de SGSI, y significa lo siguiente:

- **Plan** (Establecer el SGSI): Implica, establecer a política del SGSI, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.
- **Do** (Implementar y operar el GSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.
- **Check** (Monitorizar y revisar el SGSI): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- **Act** (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI.

PLAN	Establecer SGSI.	Definir las métricas.
DO	Implementar y Operar el SGSI.	Implantar las métricas.
CHECK	Supervisar y Revisar el SGSI.	Revisar los datos de las métricas.
ACT	Mantener y Mejorar el SGSI.	Revisar/Mejorar las métricas.

Esta era la parte que nos interesaba presentar de la norma original, pues es la base del concepto de "Ciclo de vida", título del capítulo. Ahora seguiremos adelante con la versión UNE-EN ISO/IEC 27001 de Mayo 2017.

No podemos presentar en el libro la norma con todo detalle (*aunque merece la pena conocerla y analizarla a fondo, recomendamos que quien tenga acceso lo haga*) pues la misma tiene sus derechos reservados, pero haremos referencia a los párrafos que nos interesan conceptualmente para abordar el ciclo de vida con máxima rigurosidad, pues según nuestra opinión, este es el concepto más importante de seguridad a lo largo del tiempo. No sirve de nada hacer un gran esfuerzo y gasto en un momento dado, si luego no se mantiene, el envejecimiento de la ciberseguridad en el siglo XXI es más vertiginoso que nunca, y un nivel alcanzado, por máximo que sea en una fecha determinada, meses después si no se mantiene sufre una degradación abismal.

Esta última versión de la norma expone con toda claridad este concepto desde su inicio:

En su punto 0 Introducción, 0.1 Generalidades, presenta:

> "*Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información*".

Continúa haciendo referencia al análisis de riesgo y al liderazgo y compromiso de la dirección, asegurando , apoyando y siguiendo permanentemente el SGSI.

Nos interesa también hacer referencia a los puntos:

6 Planificación, 6.1 Acciones para tratar los riesgos y oportunidades, 6.1.1 Consideraciones generales

Que describen:

a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y

2) evaluar la eficacia de estas acciones.

Luego describa más en detalle el análisis de riesgo, la concienciación, la planificación y la evaluación del desempeño, punto sobre el cual también presentamos aspectos relevantes: 9 Evaluación del desempeño, 9.1 Seguimiento, medición, análisis y evaluación:

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos;

NOTA Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

c) cuándo se deben llevar a cabo el seguimiento y la medición;

d) quién debe hacer el seguimiento y la medición;

e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;

f) quién debe analizar y evaluar esos resultados.

Continúa describiendo la necesidad de "Auditorías Internas" y cómo debe ser la "Revisión por la dirección", finalizando con el punto 10.2 Mejora continua.

Este brevísimo resumen que hemos presentado sobre el estándar ISO/ UNE 27001, tiene la única intención de despertar consciencia sobre la importancia de la "Mejora continua" de la Ciberseguridad, y en particular cómo se debe llevar a cabo este proceso, el cuál como acabamos de presentar, debe responder a una planificación, medición (concreta y cuantificable) y evaluación de resultados para poder adoptar acciones de mejora. Esto es la razón de ser de un "Ciclo de vida" y la mejor forma de implementarlo es poder definir un robusto sistema de "métricas" que nos permitirá ir midiendo el grado de avance sobre los objetivos de control que nos hayamos planteados.

Para comprender y ejecutar estas métricas, nuevamente nada mejor que basarnos una vez más en estándares, así que seguiremos adelante en este capítulo, ahora con la norma **ISO/IEC 27004**.

Cabe mencionar que existen dos estándares más que se pueden tener en cuenta para la implementación de métricas de seguridad, estos son del **NIST** (National Institute of Standards and Technology), el **NIST 800–55** "Security Metrics Guide for Information Technology Systems" y el **NIST 800–80** "Guide for Developing Performance Metrics for Information Security".

10.1. Presentación del estándar ISO/IEC 27004.

Esta norma fue publicada el 15 de diciembre de 2009 y su última revisión fue en año 2016.

Como venimos intentando remarcar, uno de los aspectos mas importantes que se debe destacar del estándar ISO 27001, es la importancia que hace sobre el carácter "medible de los controles". En concreto, si un control no se puede medir, entonces no nos aporta absolutamente nada al SGSI. Ahora bien, ¿cómo debemos medir esos controles?, es aquí donde entra en juego el estándar ISO/IEC 27004, y como se verá en estas líneas, aporta un gran valor agregado en el momento de comenzar a implementar

esta norma, pues desde el inicio, se comienzan a pensar todas las fases de la misma bajo el concepto de "Medición".

NOTA: Para poder comprender con claridad el sentido, los conceptos y definiciones que aquí se desarrollarán, es recomendable leer previamente los artículos que se han publicado en su momento respecto a esta familia de estándares, todos ellos pueden aún descargarse gratuitamente de la página Web "www.darFe.es":

www.darFe.es: Menú: Descargas -> Tecnologías de la Información -> Nuevas Descargas

https://darfe.es/es/nuevas-descargas/category/4-tec

- ISO-27001 - Los controles (Parte I)
- ISO-27001 - Los controles (Parte II)
- ISO-27001 e ISO-27004
- Análisis de ISO-27001:2005
- Esquema Nacional de Seguridad e ISO 27001, ¿Cómo implantar ambos en mi empresa?
- ANÁLISIS DE ISO-27001-2005 ays_Nro4_jul-ago_2006
- ANÁLISIS DE ISO-27001-2005 (Resumen) ays_Nro5_sep-oct_2006
- Analisis ISO 27001 Secutiy_&_Technology nov-dic_2006
- ISO-27001 e ISO-27004 ays_Nro9_abr2007
- ISO-27001 y las PyMEs ays_Nro13_sep-2007
- Problemática-ventajas y desventajas de ISO-27001 en PyMEs ays_Nro14_oct-2007
- ISO 20000 o ISO 27000 ays_Nro16_nov_2007-Nro_especial
- Metodología de Implantación y Certificación en las Pymes (ISO-27001) ays_Nro17
- ISO–27001, y las AAPP ays_Nro18_2008

- ISO–IEC 27001-2005 & LOPD 1 ays_Nro19_2008
- ISO–IEC 27001-2005 & LOPD 2 ays_Nro20_2008 Versión:01
- Métricas de Seguridad-Indicadores y Cuadros de Mando ays_Nro21_2008
- Auditoria Interna en ISO-27001 ays_Nro22_2008

Volviendo a ISO/UNE 27004, como se irá viendo a lo largo de este capítulo, la idea de medición es muy amplia y en definitiva, va desde la medición más simple hasta la combinación de varios niveles o instancias de ellas para poder ofrecer datos que lleven a un verdadero "cuadro de mando de la seguridad", que sería el objetivo último de todo el SGSI, y a través del cual, los diferentes niveles jerárquicos de la organización, podrán acceder a la información de seguridad, que a su nivel le hace falta conocer y en base a esta adoptar las decisiones correspondientes.

La norma ISO 27004, comienza con una Introducción, de la que se debe destacar:

> *"El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras".*

El segundo apartado define el **ámbito**, como una guía sobre la especificación y uso de técnicas de medición, para proveer precisión en la observación del SGSI en cualquier tipo de organizaciones y con el propósito de crear una base para recolectar, analizar y comunicar datos relacionados a este SGSI, los cuales serán empleados para tomar decisiones que permitan mejorar el mismo.

Hace referencia a que es indispensable para la aplicación de este documento, el conocimiento del estándar ISO 27001.

10.2. Terminología.

A continuación sólo se describen las definiciones fundamentales que serán empleadas en este capítulo.

Atributo: Propiedad o característica de una "entidad", que puede ser distinguida cuantitativa o cualitativamente, por una persona o sistema automatizado.

Entidad: Un objeto (tangible o intangible), que será caracterizado a través de la medición de sus "atributos".

Indicador: Es una medida que provee una estimación o evaluación de un "atributo" especificado, con respecto a las necesidades de información definidas.

10.3. Resumen de la norma ISO 27004.

Mediciones en un SGSGI:

Se basa sobre el modelo PDCA (Plan – Do – Check – Act) que ya hemos hablado. Se podría resumir esto en la idea que, las mediciones están orientadas principalmente al "**Do**" (Implementación y operación de SGSI), como una entrada para el "**Check**" (Monitorizar y revisar), y de esta forma poder adoptar decisiones de mejora del SGSI a través del "**Act**"

Una organización debe describir cómo se ínter relacionan e interactúan el **SGSI** y **las mediciones**, desarrollando guías que aseguren, aclaren y documenten esta relación, con todo el detalle posible.

Los objetivos de estos procesos de mediciones son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del SGSI, incluyendo continuas mejoras.
- Proveer estados de seguridad que guíen las revisiones del SGSI, facilitando mejoras a la seguridad y nuevas entradas para auditar.
- Comunicar valores de seguridad a la organización.

- Servir como entradas al plan de análisis y tratamiento de riesgos.

El modelo y método para las mediciones de seguridad:

Se debe desarrollar un programa de cómo ejecutar la medición de la seguridad de la información. El éxito de este programa, se basará en la asistencia o ayuda que estas mediciones aporten para adoptar decisiones, o determinar la eficiencia de los controles de seguridad. Por lo tanto este programa de mediciones debe estar basado en un "**Modelo**" de mediciones de seguridad de la información.

Este Modelo es una estructura que enlaza los *atributos* medibles con una *entidad* relevante. Estas entidades, incluyen procesos, productos, proyectos y recursos. Es decir, este modelo debe describir **cómo** estos atributos son cuantificados y convertidos a *indicadores* que provean bases para la toma de decisiones, sustentados en necesidades de información específica.

El primer paso para el desarrollo de este modelo, es definir los atributos que se consideran más relevantes para medir la información que se necesita. Un mismo atributo puede ser incorporado en múltiples mediciones, soportando diferentes necesidades de información.

Para definir **cómo** los atributos deben ser medidos, esta norma propone también un Método.

Existen dos tipos de métodos para cuantificar los atributos:

- Subjetivos: Implica el criterio humano.
- Objetivos: Se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son:

- Encuestas/indagaciones.
- Observación.
- Cuestionarios.

- Valoración de conocimientos.
- Inspecciones.
- Re-ejecuciones.
- Consulta a sistemas.
- Monitorización ("Testing")
- Muestreo.

Un tema a considerar es la asociación de mediciones con determinadas escalas, de las cuales se proponen los siguiente tipos:

- Nominal: Los valores son categóricos.
- Ordinal: Los valores son ordenados.
- Intervalos: Se poseen máximos y mínimos con distancias entre ellos.
- Ratio: Tienen escalas de distancias, relacionadas a mediciones.

La última referencia la hace respecto a la unidades de medición, recomendando emplear convenciones para uniformar las mismas

El último aspecto a considerar aquí es el de la **frecuencia**. Se deberían definir y programar claramente los intervalos en los cuales se llevará a cabo cada medición (Semanal, mensual, trimestral, anual, etc.). Considerando una relación entre la necesidad de contar con esta información y el esfuerzo para obtenerla (coste/beneficio).

Definición y selección de las mediciones en un SGSI:

La norma especifica también, cómo desarrollar las mediciones para poder cuantificar la eficiencia de un SGSI, sus procesos y controles.

La mediciones de la información pueden ser requeridas para:

- Gobierno Corporativo.
- Cumplimiento de regulaciones y/o requisitos legales.
- Operaciones o gestión organizacional.
- Certificación de un SGSI.

- Clientes, partners, socios de negocio, etc.
- Mejoras en la implementación y/o eficiencia del SGSI.
- Mejora de procesos.

Los pasos a seguir para el establecimiento y operación de un programa de mediciones son:

- Definición de los procesos
- El desarrollo de mediciones aplicables.
- La implementación del programa.
- Revisión de mediciones.

Finalmente todo el programa de mediciones debe ser revisado en pasos posteriores (y continuos), para verificar que el mismo sigue ofreciendo a la organización información válida, las fuentes y otros atributos continúan siendo correctos y los beneficios contra el esfuerzo requerido siguen siendo positivos. Como consecuencia de este análisis, las mediciones podrán ser mantenidas, eliminadas, sustituidas o modificadas.

Las mediciones están directamente relacionadas a:

- Procesos de sistemas de gestión (Ej: ¿Se realizaron las auditorías?, ¿Este manual cumple con los estándares?, etc.).
- Ejecución de controles de seguridad de la información (Ej: Volumen de incidencias por tipo, acceso a tablas, etc.).

Esta norma define dos categorías de mediciones:

- Mediciones de ejecución: Eficiencia.
- Mediciones de progreso: Cambios en la protección de la información.

Los constantes ciclos de estas mediciones requieren inicialmente un fase de **planeamiento**, donde se establezcan las premisas genéricas, se pueda elegir una selección de mediciones de información de seguridad y su categorización. Este planeamiento garantiza que el contexto de mediciones sea correctamente establecido. El planeamiento debe incluir identificación de recursos financieros,

humanos y de infraestructura incluyendo los responsables de proveerlos y asignarlos para asegurar su correcta implementación.

Una medición para ser válida, debería cumplir con los siguientes criterios:

- Estratégico: Alineado con la estrategia y misión de seguridad de la información.
- Cuantitativo: Datos numéricos o empíricos, más que opiniones.
- Razonable: El valor del dato recolectado no debería ser mayor al coste de recolectarlo.
- Verificable: Cualquier revisión por parte de un tercero, debería ser capaz de valorar el dato y obtener resultados.
- Tendencia: Los datos deberían ser representativos del impacto, cada vez que se imponen cambios.
- Usable: Los resultados deberían apoyar la toma de decisiones.
- Indivisible: Los datos deberían ser recolectados al más bajo nivel de desagregación posible.
- Bien definido: Bien documentadas sus características como frecuencia, fórmula, evidencia e indicadores.

Para seleccionar los controles adecuados, las organizaciones deberían realizar los siguientes pasos:

- Definir un programa (como se mencionó en los puntos anteriores).
- Seleccionar los objetivos de control y los controles a ser incluidos en las mediciones.
- Definir los indicadores para los controles seleccionados.

Las mediciones seleccionadas deberían reflejar la prioridad de la información que se necesita, las mismas deben ser documentadas. Ejemplos de ellas las presenta en el ANEXO A de la norma.

Se presentan a continuación campos que pueden contemplar:

- Nombre.
- Propósito.

- Tipo de propósito.
- Ámbito o dominio.
- Método de medición.
- Escala.
- Roles.
- Método de recolección de datos.
- Ciclo de vida.
- Criterio.
- Campos del indicador: Efectos de impacto, causas de desvío, gráficas.

La organización debe documentar su plan para la implementación de las mediciones de seguridad de la información y llevar adelante el mismo. Esta implementación podría contemplar:

- Listado de mediciones a ser recolectadas y empleadas, incluyendo sus especificaciones.
- Definición de pasos para recolección y análisis de los datos medidos.
- Identificación de formatos de reporte para cada medición.
- Definir un ciclo de refresco de las mediciones para asegurar su corrección en relación al SGSI.

Operación de las mediciones del SGSI (Fase DO: Hacer)

Las mediciones deben encontrarse totalmente integradas al SGSI incluyendo:

- Definición y documentación de roles y responsabilidades que participan en el desarrollo, implementación y mantenimiento de las mediciones dentro del contexto del SGSI.
- Políticas y procedimientos que definan el empleo de las mediciones en la organización, difusión de la información medida, auditoría y revisión de los procesos de medición.
- Procesos de monitorización de las mediciones para evaluar su uso.

- Procesos de eliminación, modificación y adición de nuevas mediciones, para asegurar que las mismas envuelven a toda la organización.

La fase "Do" es una de las que establece el enlace entre las mediciones que resultan adecuadas para cubrir en la organización en un momento dado. Durante esta fase, los resultados del programa de mediciones debería ser revisado y aprobado. En este momento se decidirán los recursos que se asignarán para la implementación de las mediciones. La Dirección deberá acordar este conjunto de mediciones planificadas , para lanzar las tareas con los recursos y la infraestructura correspondiente.

Mejoras de las mediciones del SGSI (Fases Check y Act: monitorizar/ auditar y actuar).

Las fases "Check" y "Act" facilitarán las mejoras y reencauces de los procesos de medición, y permitirán el análisis de la información de mediciones disponibles y su apoyo para la toma de decisiones. En todo este ciclo, las mediciones deberán ser evaluadas, ajustadas y detectadas a las necesidades del SGSI, asegurando que su evolución continúe cubriendo los objetivos de seguridad, respecto a la posición de partida del proceso.

Se debería identificar la frecuencia de estas fases, y en estos períodos realizar las revisiones y establecer los mecanismos para hacer posible la reactivación o el lanzamiento automático de fases de revisión para detectar los desvíos de las condiciones iniciales.

Este punto presenta dos aspectos:

1) Definir un criterio para evaluar la información (Análisis de información).
2) Definir un criterio para evaluar el proceso de mediciones (Validación de mediciones).

Las mediciones deberían ser revisadas, cuando ocurran cambios en la organización. Para asegurar que las mediciones reflejan el estado actual de seguridad, es importante verificar que los datos siguen siendo válidos. Las revisiones se deben realizar también a intervalos planeados, para verificar si se siguen ejecutando tal cual se diseñó en

su momento. También se recomienda la realización de evaluaciones externas para proveer una visión independiente del programa.

El propósito de estas revisiones es asegurar que:

- Las mediciones son correctamente revisadas al ocurrir cambios en los objetivos de negocio.
- Las mediciones que no se suelen emplear son quitadas e ingresan nuevas mediciones necesarias.
- Los recursos que soportan estas mediciones son los adecuados.
- Las decisiones sean documentadas para permitir futuras comparaciones, o analizar tendencias.

Los resultados de estas mediciones deberían ser difundidos a todo el personal interesado, directivos, gerentes, técnicos y personal relacionado a la seguridad. El formato de estos reportes debe ser acorde a las necesidades de cada grupo o perfil al que va dirigido e informar los aspectos que cada uno necesita, con el grado de detalle adecuado a su función o rol en la organización.

Algunos ejemplos de reportes se presentan en el ANEXO A de la norma. Se debe considerar la confección de reportes internos y externos a la organización con las restricciones pertinentes en cada caso, controlando y auditando con máxima precaución lo que se difundirá externamente.

Es muy importante que estos reportes faciliten la "realimentación" de información, basada en lo que puedan aportar sus consumidores, y generar los mecanismos necesarios para analizar e implementar este ciclo de retorno.

La dirección.

La Dirección debería establecer y mantener acuerdos en sus mediciones. Su implementación debe ser acorde a lo que establecen los estándares internacionales, teniendo en cuenta la aceptación de los requerimientos de mediciones.

- Deberán establecerse acuerdos entre la Dirección y el personal que llevará adelante esta tarea de mediciones. Demostrando el

interés de todos los niveles de la organización, por ejemplo a través de mediciones en la política de seguridad, asignación de responsabilidades, servicios, preparación, presupuesto y recursos.

- Todos los acuerdos deberían ser comunicados a la organización.

La Dirección deberá proveer evidencias de estos acuerdos, de su implementación, operación, revisión, monitorización, mantenimiento y mejora de todo el programa de mediciones a través de:

- Establecimiento del programa de mediciones.
- Asegurar que el programa sea implementado.
- Establecer roles y responsabilidades en el programa de mediciones.
- Comunicar a todo el personal interviniente el programa de mediciones y sus indicadores de progreso.
- Proveer suficientes recursos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el programa de mediciones.
- Asegurar que las auditorías internas del programa de mediciones, como una parte de las auditorías SGSI, sean las correctas.
- Las revisiones del programa de mediciones sean parte del SGSI

La dirección deberá asignar y proveer los recursos para el programa de mediciones, incluyendo los responsables de todos los aspectos y la infraestructura para llevar adelante sus funciones.

La dirección deberá asignar los siguientes roles y responsabilidades para la ejecución y uso de las mediciones:

- Propietario de la medición.
- Persona o unidad responsable del requerimiento de mediciones.
- Persona o unidad responsable de recolectar y almacenar los atributos de información de una entidad objeto de medición.
- Persona o unidad responsable de la comunicación a la organización, de la importancia del programa de mediciones y sus resultados, para asegurar su aceptación y empleo.

- Persona o unidad responsable de la evaluación del programa de mediciones, para asegurar que se corresponde con los controles de seguridad.
- Personas que intervienen y dirigen el programa de mediciones.

Será necesario establecer autorizaciones, certificaciones y/o acreditaciones al personal que llevará a cabo estas tareas y los criterios para la formación técnica de los mismos, como así también la capacitación de todo el personal interviniente, respecto a los temas fundamentales que envuelve el proceso de mediciones.

La dirección deberá asegurar que todo el personal sea consciente de lo relevante e importante que es el programa de mediciones y cómo cada uno de ellos contribuyen a mejorar estos objetivos del SGSI.

Conclusiones finales.

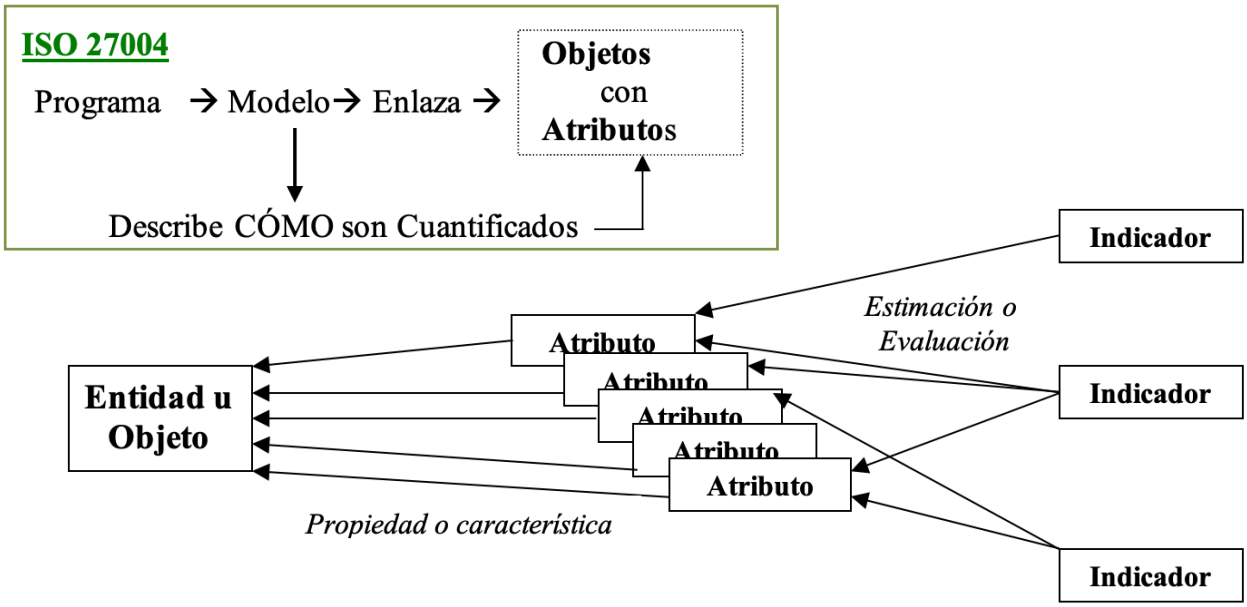
En este capítulo, se trató fundamentalmente de demostrar que es importante "Medir el SGSI", y de hacerlo, la norma ISO/IEC 27004, propone un lenguaje común que permite seguir avanzando de la mano de la normalización.

Tal vez lo más importante es que una vez más hace presente la idea de "**ciclo de vida**", pues estas mediciones también se llevan a cabo de esta forma, y justamente por ser así es que facilitan la concreción de un verdadero cuadro de mando "vivo" que ofrece la información que necesita cada nivel de la empresa.

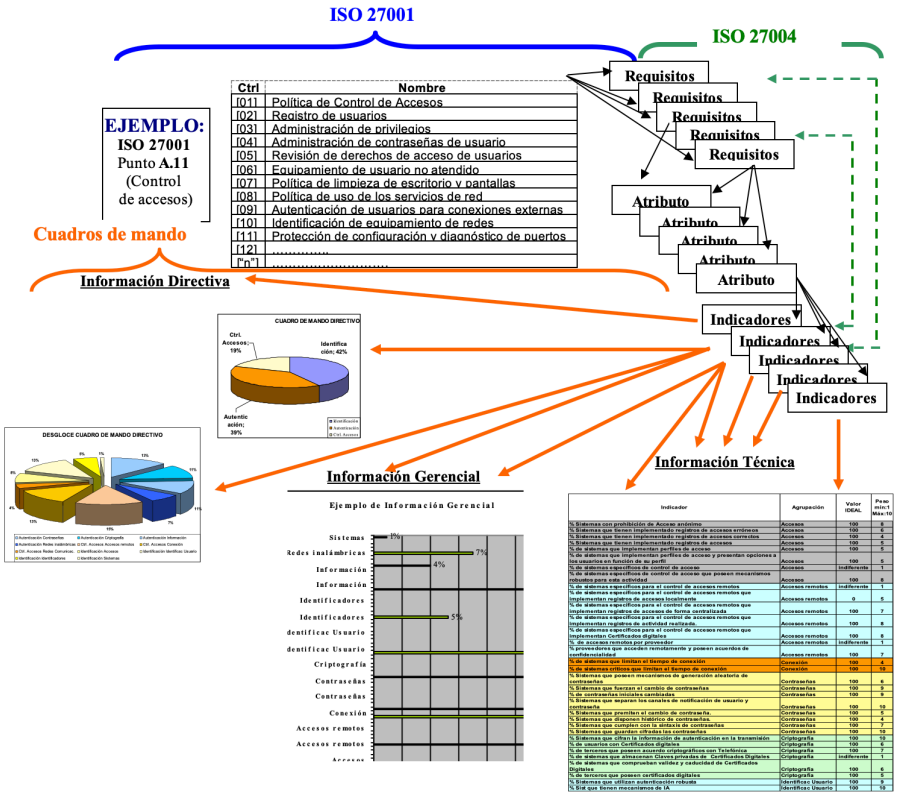
A continuación se presenta en forma esquemática lo que se puede llevar a cabo a través de la combinación de ISO 27001 e ISO 27004. Desde la definición de los controles, requerimientos, atributos e indicadores, para llegar finalmente a los niveles de agrupamiento/desagregación de información que mas se desee.

Como se fue desarrollando, esta norma nos describe cómo cuantificamos "**Objetos**" con sus respectivos "**Atributos**".

Los indicadores nos permitirán realizar esta evaluación.



Por lo tanto, si tenemos bien definidos los "**Controles**", y luego en el "**Análisis de riesgo**" identificamos cuáles son los "**activos críticos**". Si a cada uno de ellos los evaluamos respecto al nivel de "**Resiliencia**" que poseen, ahora podemos establecer el sistema de "**Medición**" y generar con ello un "**Cuadro de Mando**" que nos permita ejecutar con precisión ese ciclo "**Plan - Do - Check - Act**", siguiendo y manteniendo "Viva" nuestra **Estrategia de Resiliencia**.

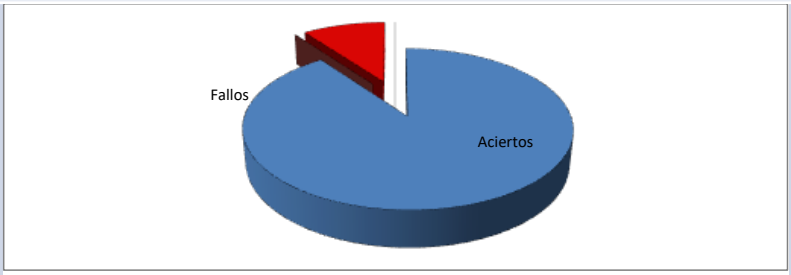


A continuación, se presenta un ejemplo de cómo puede ser definido un formato para estas métricas.

MÉTRICAS E INDICADORES	
FORMATO DE INDICADOR DE SEGURIDAD	
MEDIDA	Nombre de la métrica.
DATOS ADJUNTOS	Posibilidad de adjuntar algún fichero (**OPCIONAL**).
VALOR	Define la cantidad medida como un porcentaje, número, frecuencia, coeficiente, diferencia…
CÓDIGO	Número que identifica a la métrica.
TIPO	Tipo de control al que se refiere la métrica. Puede ser de despliegue, de eficacia, de eficiencia…
PROPÓSITO	Objetivo que se persigue con esta métrica.
MÉTODO DE MEDIDA	Define el método utilizado en la medida, la función de cálculo o el modelo de análisis.
ESCALA	Define el tipo de escala (nominal, ordinal, intervalos, ratio…).
PROCEDIMIENTO	Define el método de recolección de datos utilizado en la métrica.
FRECUENCIA DE OBTENCIÓN	Periodo de tiempo que transcurre entre la recogida de datos.
FECHA DE VALIDEZ	Fecha de expiración de la validez de la métrica.
CRITERIOS	Criterios para la medida.
ALCANCE O DOMINIO	Define el ámbito al que se circunscriben los datos que se van a recabar (una máquina específica, un servicio, un grupo de recursos, una red, un edificio, un departamento o grupo, una unidad de negocio…) (**OPCIONAL**).
COMENTARIOS	Comentarios adicionales de la métrica.
REPRESENTACIÓN	Representación gráfica de la evolución del indicador.

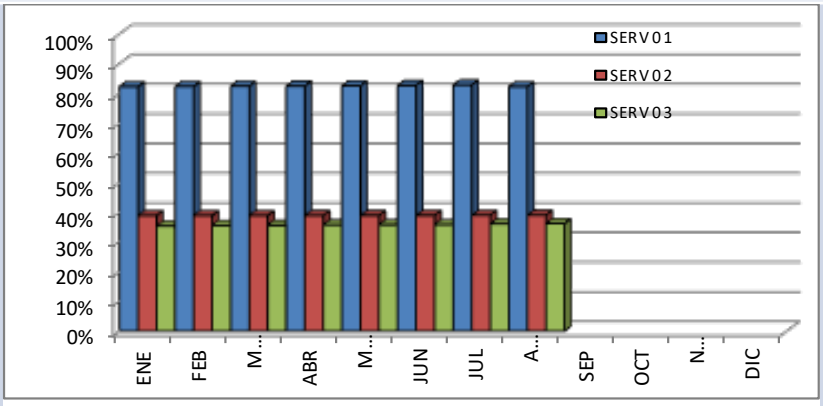
Siguiendo con ejemplos, a continuación se presentan algunos ejemplos de mediciones sobre un SGSI real.

TEST DE CONCIENCIACIÓN	
NOMBRE	Test de concienciación.
CÓDIGO	I2020_05
TIPO	Progreso.
VALOR	Porcentaje.
ESCALA	Porcentual.

PROPÓSITO		Comprobar el grado de concienciación en Seguridad de los empleados de la empresa
MÉTODO DE MEDIDA		Porcentaje total de preguntas acertadas.
PROCEDIMIENTO		Se realiza un test al personal, se corrige y se haya el porcentaje de preguntas acertadas.
CICLO DE VIDA	**FRECUENCIA DE OBTENCIÓN**	Anual.
	PERIORICIDAD DE ENTRADA	Anual.
	FECHA DE OBTENCIÓN	1/2/2020
	FECHA DE VALIDEZ	1/2/2021
CRITERIOS		Grado de concienciación Satisfactorio > 65%
ALCANCE O DOMINIO		Totalidad de la empresa.
COMENTARIOS		Se aumentará el criterio de validez en el 2021.
REPRESENTACIÓN		

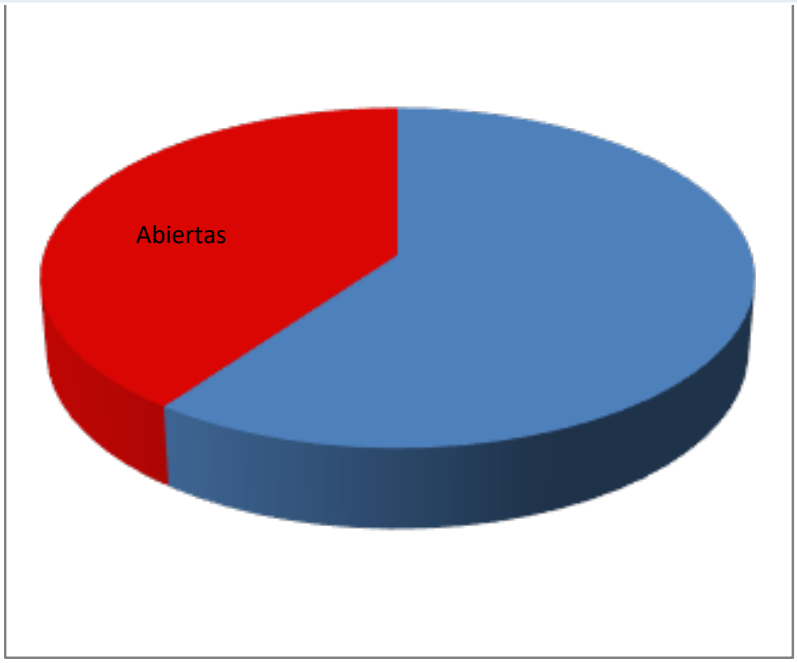
Otro ejemplo.

GESTIÓN DE LA CAPACIDAD DE LOS SERVIDORES		
NOMBRE		Gestión de la capacidad de los servidores.
CÓDIGO		I2020_09
TIPO		Eficiencia.
VALOR		Porcentaje.
ESCALA		Porcentual.
PROPÓSITO		Comprobar la gestión de capacidad de los servidores para la planificación de estos a medio plazo.
MÉTODO DE MEDIDA		Porcentaje de ocupacion de estos mensual.
PROCEDIMIENTO		A final de mes se calcula en porcentaje de ocupación de los servidores.
CICLO DE VIDA	**FRECUENCIA DE OBTENCIÓN**	1 vez al mes.
	PERIORICIDAD DE ENTRADA	Mensual.
	FECHA DE OBTENCIÓN	Mensual.

	FECHA DE VALIDEZ	Anual.
CRITERIOS		Planificar ampliación a partir del 85% de capacidad.
ALCANCE O DOMINIO		Servidores de gran capacidad.
COMENTARIOS		Cuando uno de los servidores supere el 85% pasará a tener color ROJO.
REPRESENTACIÓN		

Otro ejemplo.

INCIDENCIAS ABIERTAS/CERRADAS		
NOMBRE		Incidencias Abiertas/Cerradas.
CÓDIGO		I2020_17
TIPO		Métrica de Eficiencia.
VALOR		Número.
ESCALA		Ordinal.
PROPÓSITO		Comprobar la capacidad de resolución de las incidencias de seguridad.
MÉTODO DE MEDIDA		Nº de incidencias abiertas Nº de incidencias cerradas.
PROCEDIMIENTO		Mensualmente se verán las incidencias abiertas y las cerradas, se irán sumando incrementalmente a lo largo del año, tanto las abiertas como las cerradas.
CICLO DE VIDA	**FRECUENCIA DE OBTENCIÓN**	Mensual.
	PERIORICIDAD DE ENTRADA	Mensual o cuando ocurra una incidencia o se resuelva.
	FECHA DE OBTENCIÓN	Mensual o cuando ocurra una incidencia o se resuelva.
	FECHA DE VALIDEZ	Anual.
CRITERIOS VALIDEZ		Las incidencias abiertas no deben superar mas de un 25% a final de año. (Se estudiará el caso, si el nº de incidencias abiertas en pequeño)
ALCANCE O DOMINIO		Sistema de Incidencias de Seguridad.

COMENTARIOS	Se revisará los criterios de validez en 2021.
REPRESENTACIÓN	

Se ha intentado representar una pequeña muestra de este tipo de mediciones para dejar como ejemplo lo que expone la norma ISO/IEC 27004, y a su vez como se relaciona la misma con la ISO/UNE 27001 anteriormente presentada y, de esta forma dejar el camino abierto para unificar todo en un "**Cuadro de Mando**" que nos permita realizar un seguimiento detallado del "Ciclo de Vida" de la Ciberseguridad o del estado de avance y cumplimiento de toda esta "**Estrategia de Resiliencia**" que estamos exponiendo en estos capítulos anteriores. El hecho concreto es poder contar con diseños y herramientas sólidas que evalúen y puedan cuantificar objetivamente todo el planeamiento realizado y verificar o generar las alarmas necesarias ante cualquier desvío.

Tened siempre presentes las diez reflexiones sobre resiliencia con que partimos todo este análisis, las cuáles junto con el análisis de riesgo y la matriz de resiliencia nos permitieron llegar hasta aquí. Ahora es el momento en el cual podemos dar por iniciado nuestro primer rodaje de este "**ciclo de vida**" y demostrara a la dirección el grado de cumplimiento, o no del curso de acción que se ha definido.

Esto último tal vez sea uno de los puntos clave de todo este trabajo, pues si bien nuestra estrategia de Ciber resiliencia pueda ser calificada como óptima en cualquier foro o por cualquier técnico, si la dirección no es consciente de este hecho, dejará de aportar su invalorable apoyo, y sin el

mismo a lo largo de los ciclos de vida, nuestro diseño se vendrá abajo, pues sin el convencimiento y el involucramiento de la dirección, ya nos lo dice al principio de la norma 27001, esto no sirve de nada. La mejor forma de mantener interesada a la dirección es con rigurosas y creíbles mediciones, y con cuadros de mando del ciclo de vida de nuestra estrategia de Ciberdefensa.

11. Proactividad Forense.

Este capítulo lo considero uno de los más importantes del libro. En primer lugar por ser un concepto nuevo que estoy proponiendo y del que creo que no se ha desarrollado aún en la bibliografía informática y de telecomunicaciones. En segundo lugar, porque he sufrido ya varias veces los graves inconvenientes de realizar un análisis forense sobre empresas que JAMÁS habían tomado medidas previas sobre esta realidad.

La experiencia nos ha demostrado desde hace varios años que ante emergencias concretas o crisis, el cerebro humano no suele funcionar del todo bien. Las prisas y nervios no son buenas consejeras, y en general ocasionan más daños que beneficios. Todo esto viene a cuento porque ya nos ha sucedido en reiteradas oportunidades que al acontecer un incidente, y muchas veces con la mejor buena intención, se apagan sistemas, desconectan cables, se desactivan routers o switches, extraen dispositivos de almacenamiento o impresión, etc. Este tipo de acciones, si no han sido aprobadas, reguladas, autorizadas y documentadas, NO deberían realizarse, y mucho menos con prisas y sin escalarlas adecuadamente, pues llegado el momento de obtener información del incidente nos resulta imposible reconstruir lo sucedido, con lo que nos quedamos sin saber qué pasó y, peor aún, cómo poder erradicarlo.

Algo que siempre me ha llamado la atención, es que e origen del nombre "análisis forense" en la mayoría de los casos lo asociamos a delitos policiales, de los cuáles, en la mayoría de series o películas, debido a gravedad e importancia del hecho, se relacionan con muertes u homicidios. Es decir, se lleva a cabo con un hecho que ya ha finalizado. La investigación forense en el caso informático y de telecomunicaciones, no necesariamente debe ser así, y de hecho he vivido ya algunas experiencias de "convivir con el enemigo" y con ello poder comenzar una investigación durante el desarrollo del incidente mismo, y hasta llegar a evitarlo.

Cualquiera podría pensar que el concepto que acabo de citar, entonces, no es análisis forense. Probablemente tenga razón, pero lo que sí es significativo, llamémoslo como mejor nos guste, es que las técnicas comparten mucho en común. Como veremos a lo largo de este capítulo, lo más importante es poder contar con todo lo necesario para que este trabajo sea un éxito. Durante el incidente, o a posteriori lo que deseo remarcar es

que si no vamos realizando un trabajo responsable de actividad previa, preparación y capacitación, el resultado final de un incidente será nefasto.

Este conjunto de medidas y acciones es lo que he llamado "**proactividad forense**".

Proactividad forense.
Conjunto de medidas y acciones imprescindibles de preparación forense.

Se trata de un concepto que estoy proponiendo y lo considero de suma importancia, pues, es imprescindible si buscamos una infraestructura ciberresiliente, que estemos en capacidad de realizar un análisis forense en las mejores condiciones posibles. La proactividad forense, es el conjunto de medidas previas que, si no las tuve en cuenta, luego se dificultará o hará imposible esta actividad.

El concepto clásico de informática forense es : "ciencia que se encarga de asegurar, identificar, preservar, analizar y presentar un conjunto de datos, también llamados, prueba digital, de tal modo que ésta pueda llegar a ser aceptada en un proceso legal y/o judicial, cuyos fines son:

- Preventivos
- Correctivos
- Probatorios
- Auditores

Estos fines, como bien están expresados, responden a una serie de pasos y hasta podemos pensar en cierto orden de los mismos, por lo que es necesario realizar mucho trabajo previo para ello, esto es lo que se intentará definir en este capítulo como: proactividad forense.

Yendo siempre hacia nuestros estándares internacionales, considero que esta proactividad forense debe estar guiada principalmente por el estándar **ISO/IEC 27037**:2012 "Guía para la identificación, recolección, adquisición y preservación de evidencias"

De esta norma, llegado el momento de una análisis forense, desearía rescatar lo siguiente:

1ª Fase: Asegurar la escena. (Medidas físicas, horarias, periféricos, conexiones/desconexiones eléctricas y de red).

2ª Fase: Recolección de evidencias (Identificación y recolección) de +Volátil **—>** -Volátil.

—> Registros, caché. Tabla de enrutamiento, Caché ARP, tabla de procesos, estadísticas del kernel, la memoria.

—> Archivos temporales. Discos. Logs. Configuración física y topología de red. Documentación.

Recolección: Fuente datos original:

1ª Copia (Hash - Judicial) Se compara su Hash con el de la fuente

2ª Copia (Hash – Respaldo Laboratorio)

3ª Copia (Hash – trabajo en laboratorio)

Ideas clave para la recolección de evidencias:

- Fuentes de información (*Registros, Logs, IDSs, sondas, Honey Pots, Sistemas de autenticación y control de accesos, máquinas de salto, configuraciones, gestores documentales, sistemas de control de integridad, sistemas de backups*).
- Mantenimiento de la integridad y cadena de custodia.
  - Asegurar que la evidencia no ha sido alterada.
  - ¿Podemos garantizarlo? (*Hash, copias bit a bit, imágenes de discos y sistemas, sincronismos y sellados de tiempo, redundancia de Logs, protección física, procedimientos*)
- Volatilidad (*Memoria RAM - Procesos - Conexiones de red*)
  - Si los dispositivos se apagan (perdemos lo volátil)
  - Si los dispositivos no se apagan (se puede alterar la evidencia)… *Compromiso*.
- Coordinación con fuerzas judiciales y policiales.

3ª Fase: Preservación de las evidencias (Una mala preservación puede invalidar toda la investigación).

4ª Fase: Análisis de las evidencias.

Se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

5ª Fase: Informes. (Informe ejecutivo - Informe técnico)

CONCLUSIONES:

- Trabajo realizado
- Posibles soluciones
- Responsables e hitos
- Acciones de mejora
- Revisiones

Otras normas que también pueden ser tenidas en cuenta son:

- **RFC 3227** "Guidelines for Evidence Collection and Archiving"

  Recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.
- **UNE 71505** Gestión de evidencias electrónicas
- **UNE 71506** Metodología para el análisis forense de las evidencias electrónicas

Estas dos últimas normas, publicadas por la Asociación Española de Normalización y Certificación (**AENOR**) tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Cuando hablamos de "proactividad forense", según mi criterio, se trata de un conjunto de medidas que deben ser abordadas desde el inicio mismo

del desarrollo e implementación de nuestras redes y sistemas, bajo la hipótesis cierta que algún día deberemos realizar esta actividad y por lo tanto cuantas mayores precauciones y previsiones tengamos, sin lugar a dudas más eficiente será nuestro análisis cuando nos llegue el momento.

Mi propuesta, es que al menos sean:

- Adecuada gestión, rotación y exportación de Logs.
- Implantación de un SIEM (Security Information and Event Management).
- Medidas de salvaguardas de la integridad de la información.
- Cadena de custodia de la información.
- Control de fugas de información.
- Herramientas y prácticas de cifrado y ruptura de contraseñas.
- Herramientas y prácticas de recuperación de cachés de navegación y mensajería.
- Herramientas de sellado de tiempos (de ser posible con validez legal).
- Estricta sincronización de tiempos de toda la infraestructura.
- Contacto previo con autoridades gubernamentales, judiciales, policiales, mediáticas y notariales.
- Previsiones en la implantación y gestión de "honey Pots".
- Claros inventarios y mapas de red y sistemas de TI.
- Mecanismos robustos de control de propietarios de activos.
- Adecuadas medidas de autenticación y control de accesos que eviten el empleo de cuentas genéricas y minimicen o controles las privilegiadas.
- Mecanismos de control de la integridad de la información clasificada.
- Plataformas de captura y análisis de tráfico.
- Herramientas de recuperación de información borrada.
- Redacción de un procedimiento sencillo y claro de actividades forenses.

- Modelos predefinidos de formularios y reportes técnicos de análisis forense.
- Formación del personal en gestión de incidentes.

Desarrollemos con un poco más de detalle cada una de las mismas.

- Adecuada gestión, rotación y exportación de Logs.

  Los Logs (o registros) son la fuente principal de un análisis forense. En primer lugar se debe ser muy estricto con qué tipo de Logs son necesarios y suficientes, y luego definir una plataforma de centralización de Logs que permita recibir los Logs que exporta cada dispositivo, servidor o servicio crítico. Recordemos siempre que un intruso hará todo lo posible por borrar todas las huellas que va dejando.

  Un ejemplo que siempre pongo de manifiesto, me sucedió en una infraestructura en la que había ciertos dispositivos que eran altamente críticos. Sobre estos dispositivos era tan importante la preservación de los Logs que cada uno de ellos, exportaba los logs de autenticación y acceso a una impresora de matriz de punto con formularios continuos, por supuesto ubicada en una instalación de muy difícil acceso físico. Esta medida, creo que es el mayor ejemplo de la importancia de esta actividad pues, como el lector comprenderá, una vez que se imprimía una línea en ese formulario, el proceso es irreversible y ningún intruso lógico en cualquiera de estos dispositivos podría borrar esa huella.

- Implantación de un SIEM (Security Information and Event Management).

  Este tipo de tecnologías, cada día se va imponiendo mas como una necesidad en arquitecturas de red y TI. Existen varios productos de mercado al respecto, y por supuesto mucho software open source. Debemos considerar que cualquier despliegue informático hoy en día, genera un alto volumen de Logs, por pequeña que sea nuestra empresa. El análisis "manual" de ellos, es prácticamente imposible, por lo que este tipo de herramientas, ofrecen un alto

valor agregado, si somos creativos y prácticos pueden configurarse adecuadamente para que el volumen y capacidad de procesamiento no sea tan complicado.

- Medidas de salvaguardas de la integridad de la información.

  Existen diferentes herramientas que nos permiten llevar el control de cambios o control de integridad en la información, en particular esto es importante en las configuraciones de dispositivos críticos y en la información clasificada.

  Independientemente de la importancia que tiene este control de integridad en el día a día de la organización, a la hora de un análisis forense es fundamental para poder determinar con máxima precisión qué cosas han sido modificadas, y en qué intervalos de tiempo.

- Cadena de custodia de la información.

  La cadena de custodia de la información, nos permite identificar los propietarios, responsables y quién trata con la misma en cualquier instante de su ciclo de vida. En la actividad forense si esta cadena de custodia se gestiona correctamente, nos permite identificar cualquier desvío en el instante que lo necesitemos.

- Control de fugas de información.

  En el punto 12.4.4. Prevención de pérdidas de información, de este libro, trataremos este tema, pero ahora lo que nos interesa es poder seguir el rastro, si es que ha habido fugas de información en nuestra organización, por lo que tener adecuadamente implementados este tipo de mecanismos nos permitirá identificar con toda certeza este hecho y poder seguir el rastro de esa fuga.

- Herramientas y prácticas de cifrado y ruptura de contraseñas.

  El cifrado de la información, es una de las actividades relevantes en un análisis forense. En primer lugar, el conocimiento de funciones

"hash" (o resúmenes) para comparativas y resguardos de información es uno de los pilares a la hora de las pruebas.

En segundo lugar es muy común hoy en día el empleo de túneles y protocolos seguros para la secuencias de acceso y transporte de información que emplea un intruso, también es frecuente el empleo de almacenamiento de información cripotgrafiada para que el auténtico propietario no pueda analizar la actividad anómala.

Finalmente no podemos dejar de lado la frecuencia cada vez más alarmante de los ataques de tipo "ransomware" donde el intruso buscará aplicar toda la criptografía que esté a su alcance para dificultarnos las recuperación de nuestra información, sistemas operativos o aplicaciones.

- Herramientas y prácticas de recuperación de cachés de navegación y mensajería.

  La mayoría de los navegadores y programas de mensajería almacenan sus historiales de navegación y conversaciones, si se puede lograr recuperar los mismos, en muchas ocasiones nos dan información muy valiosa sobre la actividad que ha desarrollado esa persona con la aplicación. El ejemplo que más representa esta idea es el comando "history" en Linux, que nos dice por línea de comandos, cada acción que realizó ese usuario. En el caso de estas aplicaciones gráficas es algo similar. El conocimiento de cómo llegar a esta información, las rutas de dónde se almacena y las herramientas a emplear debe ser un paso previo muy importante a realizar.

- Herramientas de sellado de tiempos (de ser posible con validez legal).

  El sellado de tiempos es un proceso muy empleado hoy en día para dar validez a un hecho que guarda importancia temporal. El caso de contratos, acciones, o propiedad intelectual, por ejemplo, son típicos exponentes de este hecho. Legalmente no es lo mismo que un intruso haya accedido a nuestras infraestructuras, antes que la publicación del aviso legal que posterior al mismo, un empleado

previo a su despido que luego, o la descarga de un video de nuestra propiedad antes o después que el mismo haya sido liberado.

Cualquiera de estas situaciones puede tener validez legal o no, sobre la base del sellado de tiempos que se haya empleado. Existen un sinnúmero de servicios de sellado de tiempo: públicos privados, gratuitos, de pago, universitarios, etc. Este tema debería ser evaluado, preparado, practicado y ejecutado con l a suficiente anticipación como para que no sea la primera vez el día de realizar un análisis forense.

- Estricta sincronización de tiempos de toda la infraestructura.

Uno de los problemas más frecuentes que suele suceder cuando se realiza una actividad forense sobre más de un dispositivo, es que los mismos no tienen una base de tiempo común. Este problema es muy grave, pues al intentar reconstruir las secuencias, si los tiempos entre un elemento y otro difieren, cada evidencia que se trata puede conducir a errores en el análisis global. Otra consecuencia, más seria aún, es que judicialmente pierden consistencia y como es natural, estamos ofreciendo argumentos poco sólidos y sobre todo discurso a la parte contraria para desmoronar cualquier línea lógica de defensa, cualquier perito informático pondrá de manifiesto en nuestra contra esta falta de sincronización.

El protocolo natural que ofrece la pila TCP/IP es **NTP** (Network Time Protocol), el cual es sumamente sencillo de configurar y en todo país existen servidores de tiempo oficiales que pueden ser tomados como raíz (estrato "0"), y que sean la base de tiempo de toda nuestra organización. Cualquier dispositivo de red o TI puede apuntar a este estrato cero y constituirse como "estrato uno" de la empresa, al cual apuntarán el resto de los dispositivos. En el caso de tratarse de una organización con varias sedes, puede también constituirse más estratos en cada una de ellas y crear una estructura de sincronización de tiempos jerárquica que permite tener en hora todos los elementos que se deseen.

Este protocolo NTP debe ser uno de los pilares de nuestra proactividad forense, y si a su vez redactamos un procedimiento de sincronización de tiempos, que no debería tener más de dos hojas, que se sustente en un servidor de tiempos oficial de nuestro país, judicialmente tenemos una evidencia muy robusta y sin lugar a dudas nos facilitará la creación de una eficiente línea temporal si debemos reconstruir cualquier situación anómala.

- Contacto previo con autoridades gubernamentales, judiciales, policiales, mediáticas y notariales.

Uno de los aspectos a los que siempre le dedico tiempo durante las auditorías de seguridad es en verificar, de forma detallada, las cadenas de escalado del área u organización en cuestión. Suele ser uno de los aspectos en los que mayores debilidades se encuentran. Es común que al solicitarle al guardia de seguridad, su cadena de llamadas o procedimiento de incidencias, no lo tenga, esté desactualizado, o al llamar al único teléfono que conoce, este no conteste. Lo mismo suele ocurrir cuando al administrador de un elemento, se le informa de forma imprevista que se está llevando a cabo un ejercicio de simulación y acaba de perder la comunicación con su infraestructura: ¿qué debe hacer?, también es pintoresco cuando a algún cargo jerárquico del comité de crisis, se le informa que tiene toda su planta atacada por un troyano y le acaban de robar la totalidad de sus bases de datos: ¿qué pasos y quién debe informar?. Un caso extremo, y real, me sucedió cuando el CEO de una gran empresa nos autorizó a lanzar un "juego de guerra informático" sin previo aviso y centrado en la respuesta de su comité de crisis, a uno de sus altos directivos (y con el CEO por detrás) se le presentó un auditor diciendo que era de uno de los medios de comunicación más relevantes de ese país preguntando concretamente:

a. ¿qué está sucediendo?

b. ¿Cuándo ha sido detectado el incidente?

c. ¿Se ha informado ya a las autoridades pertinentes?

d. ¿Es cierto que se ha accedido a la información de sus clientes?

e. ¿Ha afectado datos personales?

Se puso claramente de manifiesto que no conocía claramente el plan de escalado, ni la cadena de llamadas, y mucho peor aún el control mediático. Gracias a Dios, el resultado de este trabajo, concluyó únicamente con un plan de mejora especialmente centrado en la concienciación y formación del personal.

Todo contacto previo es fundamental, en todo país existen NOC, SOC, CERT y CSIRT oficiales, como también organismos y fuerzas de seguridad de asesoramiento y apoyo ante incidentes de seguridad; se deba avanzar sobre los mismos desde el primer momento, no esperar a que algo suceda. Los dos aspectos finales de este punto: mediáticos y notariales, son los que permitirán que la situación pueda ser bien conducida o, todo lo contrario, que se desvirtúe totalmente algo que, quizás lo estemos conduciendo adecuadamente, pero no supimos transmitir bien el mensaje, o darle la solidez legal necesaria para llegar a buen puerto.

- Previsiones en la implantación y gestión de "honey Pots".

Este tema técnicamente ya ha sido tratado en los libros anteriores. Desde el punto de vista forense, son una de las mejores herramientas para llegar al fondo del problema, siempre y cuando hayan sido debidamente instaladas en tiempo y forma.

El primer aspecto a considerar con este tipo de herramientas es su despliegue, pues debe tratarse de un equilibrio justo entre la información que se exponga y hasta dónde puede ser expuesta la misma, por lo que para un intruso debe tratarse de un dispositivo real y concreto de nuestra infraestructura. Como es lógico, por más que parezca que es así, tampoco debemos poner en riesgo el resto de nuestras redes y sistemas, por lo que es necesario crear una zona debidamente segmentada y controlada por nosotros, pero intentando que sea transparente para alguien externo. Un buen ejemplo de la misma es el que presenta Wikipedia:

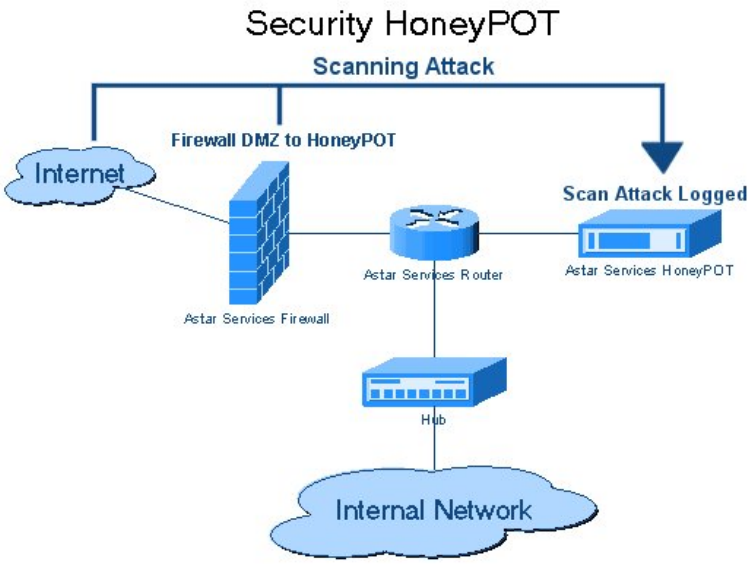


*Imagen tomada de Wikipedia (*https://es.wikipedia.org/wiki/Honeypot*)*

En la imagen anterior, podemos apreciar una arquitectura básica de implantación de un Honey Pot, en la que por medio de un firewall y un router, podemos configurar las rutas y reglas de filtrado necesarias como para nuestra red interna no corra peligro. Prestad atención al detalle del flujo representado por la flecha azul en la parte superior de la imagen, que representa el foco de nuestros análisis. Sobre ese flujo es donde podemos evaluar y aprender con todo detalle qué tipo de metodologías, herramientas, conexiones e información está empleando y buscando cualquier intruso, aspectos que a la hora de una análisis forense nos abrirán camino si este tipo de actividades evoluciona hacia nuestra infraestructura real.

Si estáis interesados en avanzar sobre este tema, os aconsejamos que comencéis por el proyecto "Honey net":

https://www.honeynet.org

Honey net Project fue fundado en 1999, se trata de una organización internacional sin fines de lucro dedicada a investigar los últimos ataques, desarrollar herramientas de seguridad de código abierto para mejorar la seguridad de Internet y educar al público sobre las amenazas a los sistemas de información.

En la actualidad ofrece varias herramientas que pueden sernos de mucha utilidad en esta proactividad forense:

- **T-POT**: Plataforma todo en uno de Honeypot. T-POT es un sistema honeypot que es fácil de implementar.
- **SNARE**: sensor honeypot de aplicación web
- **Intel Owl**: Solución de inteligencia de código abierto u OSINT para obtener datos de amenazas sobre un archivo específico.
- **Glutton**: Honeypot genérico de baja interacción.
- **Dockpot**: Honeypot SSH de alta interacción basado en Docker.
- **Conpot**: Honeypot de sistemas de control industrial de bajo nivel interactivo
- **Droidbox**: Plataforma de análisis dinámico para aplicaciones de Android.
- **Dionaea**: Honeypot de baja interacción que captura payloads (cargas útiles/contenido de los paquetes) y malware.

Existe también una página en español sobre este proyecto:

http://honeynet.org.es

- Claros inventarios y mapas de red y sistemas de TI.

No puedo sumar la cantidad de veces que me ha sucedido que los fallos de inventario han ocasionado brechas de seguridad y peor aún la incapacidad de reaccionar por desconocimiento de la propia arquitectura no dejando identificar el foco del problema. Los inventarios son uno de los mayores aspectos a tener en cuenta en ciberresiliencia.

Lo que intento transmitir es que los mapas e inventarios son como los mapas de carreteras, nadie hoy en día emprende un viaje sin su GPS, o como lo hacía antes con la guía de carreteras en papel… si no lo hiciera la probabilidad de pérdida es máxima. En redes y sistemas de TI es exactamente igual.

Es absolutamente imposible, operar adecuadamente con mis routers o firewalls si no conozco con máximo detalle la planta que tengo instalada.

El mantenimiento actualizado de mis mapas e inventarios es el pilar fundamental de una proactividad forense, no puedo dejarlo para el día en que suceda algún incidente pues será tarde.

Desde el inicio del diseño de una arquitectura de seguridad es fundamental pensarla como un "mapa o inventario" aplicándole toda la lógica que esté a nuestro alcance, más aún hoy en día, donde el crecimiento y flexibilidad de un sistema informático y de telecomunicaciones es máximo y vertiginoso.

Al respecto, siempre pongo de manifiesto la red telefónica conmutada y su relación con el sistema de numeración de cada país. Era imposible que cuando nació esta red, alguien imaginara que desencadenara unas pocas décadas después en la mayor máquina humana del mundo (pues siempre insisto en que: se trata de una sola máquina, no de varias, que une la totalidad del planeta). Sin embargo algunos visionarios sí lo tuvieron en cuenta a lo largo de este despliegue y las consecuencias técnicas de esta gente se reflejan en que, por ejemplo toda Europa tiene nueve cifras que identifican cualquier teléfono hacia los lugares más recónditos del mundo, y el caso es radicalmente opuesto en ciertos países (que lamentaría poner de mal ejemplo), en los cuáles dependiendo si deseo llamar desde línea fija o móvil, desde una provincia o estado, desde nacional o internacional, etc. se debe colocar un prefijo u otro, más o menos dígitos, un cero o varios, etc. teniendo como resultado que sea imposible da adivinar como debo hacer para lograr establecer una comunicación de extremo a extremo con ese subscriptor. Este hecho que estoy comentando, tal vez pase desapercibido por alguien que solo haya sufrido, pero no me cabe la menor duda que los clientes telefónicos de ese tipo de países y más aún a los operadores de esas redes, lo saben perfectamente y han pasado por estas peripecias.

Con las redes de datos hay algo muy similar. Cuando tengo el lujo de crear una infraestructura de telecomunicaciones desde cero, que tal cual se comenta: "Dios hizo e mundo en siete días" porque empezó de cero, pues si hubiese tenido que adaptarlo

emparcharlo, todavía lo estaría creando; si diseño la misma con imaginación y creatividad, seguramente a futuro minimizaré los problemas. Un ejemplo que también me gusta citar es el de una de ellas en las que formé parte y cuyo despliegue cubría toda un país. En la misma, jugamos bien con los tres rangos de direccionamiento privados (10.x.x.x, 172.16/31.x.x y 192.168.x.x) de forma tal que cada provincia, ciudad y ubicación respetaban una lógica determinada. Este diseño, nos fue facilitando un despliegue y flexibilidad enorme y a su vez, cuando uno observaba cualquier dirección IP, ese solo dato, nos indicaba con precisión dónde se encontraba exactamente ese host o subred. En este caso concreto, y gracias a un muy buen diseño, todos los mapas e inventarios se podían mantener actualizados y con máximo detalle sin mayores esfuerzos y, retomando el tema del análisis forense, cuando se estudiaba cualquier flujo de comunicación, se tenía la clara visión de los extremos y todo su recorrido.

Hoy en día existen un sinnúmero de herramientas para gestión de mapas e inventarios, y también pueden implementarse soluciones muy sencillas con herramientas y comandos de escaneo de redes o empleo del protocolo SNMP (Single Network Monitor Protocol) para mantener viva esta información y a su vez descubrir nuevos host dentro de la infraestructura.

Nuestra recomendación es que prestéis mucha atención a este tema de forma proactiva, pues una de las peores cosas que puede sucedernos es tener que realizar un análisis forense y durante el mismo descubrir dispositivos, direcciones IP o redes que no habíamos tenido en cuenta o ni siquiera sabíamos que existían.

- Mecanismos robustos de control de propietarios de activos.

  En general el propietario de un activo es quien posee los máximos privilegios, es decir es el "root" del mismo. El tema se complica sobre servidores en los cuáles puede suceder que cada aplicación tenga diferentes responsables, por ejemplo el sistema operativo lo administra un área, la base de datos otra, también hay un responsable de la aplicación Web y hasta pueden llegar a existir

Sistemas de Gestión BSS (Bussines Support System) para TI o llamados OSS (Operation Support System) para red, que también tienen conectividad con los mismos y capacidades de soporte o gestión, como sus nombres lo indican. Lo mismo está sucediendo en entornos de red, donde ya es común el empleo de firewalls o routers virtualizados, que se ejecutan en servidores virtuales y hasta poseen varias instancias, es decir un mismo router a su vez funciona como si fueran varios sub-routers, casos en los cuáles sus propietarios también pueden llegar a ser varios.

Me encanta el ejemplo de esos complejos vacacionales de "tiempo compartido", en los cuáles la propiedad concretamente tiene varios dueños. Suelen ser un precioso foco de conflictos en la división de responsabilidades cuando sucede algo o, alguna de las partes le dedica menos tiempo, esfuerzos o recursos que las otras pues es difícil decidir quién debe hacerse cargo u ocasionó el problema.

En nuestras redes y sistemas de "tiempo compartido" suceda algo similar, y si no se delimitan y registran debidamente sus derechos y obligaciones, pueden generarse complicadas anomalías difíciles de resolver o esclarecer cuando hay que analizarlas.

Una de las soluciones más eficientes que suelo encontrar es la robusta gestión de accesos, basados en cuentas personalizadas, con políticas estrictas de escalado de privilegios y sustentados por un buen mecanismo de gestión de Logs. Este tipo de medidas, nos permiten poder seguir el rastro con bastante precisión de cualquier tipo de actividad realizada por estos usuarios privilegiados, por supuesto si hemos sido "proactivos" en nuestro enfoque forense, pues de más está decir que reconstruir esto a posteriori, es imposible.

- Adecuadas medidas de autenticación y control de accesos que eviten el empleo de cuentas genéricas y minimicen o controles las privilegiadas.

Aunque parezca que este punto es exactamente lo mismo que el anterior, lo hemos separado intencionadamente para que sea tratado desde dos puntos de vista. En el punto anterior, nos estábamos refiriendo al dispositivo en concreto, este punto a lo que

se refiere es justamente a la infraestructura de autenticación y control de accesos sobre lo que se sustenta cada host de nuestra organización.

Es decir, la autenticación es garantizar que "es quien dice ser". Si esto lo pensamos sobre el mismo host, quien tenga la cuenta de root (o administrador) tiene todas las potestades para avalar que es él de la forma que mejor le plazca. Nuestra obligación es que no tenga tantas potestades, sino que dependa de un dispositivo externo que lo haga, y sobre el que justamente no tenga estas potestades. Las infraestructuras más frecuentes hoy en día se basan en directorios activos o **LDAP** (Lightweight Directory Access Protocol), servicios como **TACACS** (Terminal Access Controller Access Control System) o **RADIUS** (Remote Authentication Dial-In User Service), o servidores de control de acceso, tipo CITRIX; Fortinet, CiscoConnect, PulseSecure, etc.

Cuando planteamos este tipo de mecanismos de autenticación y control de accesos para llegar a los dispositivos finales, cualquier usuario de los mismos, tenga el privilegio que tuviere, deja huella de toda su conexión en los mismos, con lo que independientemente de la importancia desde el punto de vista de la ciberseguridad, también estamos preparando el terreno para cualquier tipo de análisis forense que tengamos que realizar a futuro.

- Mecanismos de control de la integridad de la información clasificada.

Para evitar confusiones, integridad de la información es: evitar modificaciones no autorizadas. En mi opinión, se trata de la definición más sencilla del concepto. Es decir quien está autorizado, puede hacerlo y el resto no. Si logro mantener este principio ahora viene una segunda componente: se debe garantizar el acceso siempre a la última modificación y no a cualquier anterior.

Algo que con toda vergüenza debo confesar me ha pasado, y justamente por esa razón he aprendido que no debo repetir, fue tomar como parte de un análisis forense cierta información que supuse era integra, cuando la realidad fue que no era así. En esa

situación, gracias a Dios, no pasó a mayores, pero sí implicó reiniciar toda la secuencia forense, pues una de esas evidencias hacía inconsistente todo el análisis.

Parecerá muy torpe de mi parte que puedan suceder cosas de este tipo, pero puedo asegurar, que a pesar de ser muy torpe de mi parte, lo he visto con mucha más frecuencia de lo habitual, cosa que limpia bastante mi consciencia. Por otro lado, si no he implementado mecanismos previos de control de integridad, no podré garantizar la misma durante la actividad forense, pues ya será tarde. Los mecanismos de control de integridad de la información deban acompañar todo el ciclo de vida de la misma, pues hasta inclusive puede suceder de tener que revertir algún cambio, seguir el hilo hasta la versión correcta y retornar "n" versiones hacia atrás, coas que solo puede hacerse con un robusto control de su ciclo de vida.

El mensaje que nos trae todo esto, y que es la razón de este punto más allá de torpezas o no, es que debo tener una estricta "proactividad" sobre este tema pues sino será imposible volver hacia a atrás o garantizar la integridad de cualquier dato, en particular cuando el mismo es crítico o clasificado.

Este tipo de medidas de control de integridad, no pensemos que aplica a documentación. El control de integridad es fundamental para toda la infraestructura: configuraciones, bases de datos, backups, aplicaciones, servidores de correo, web, de ficheros, etc.

La clave de todo esto, es nuevamente, contar con un buen análisis de riesgo que nos permite determinar con máxima certeza que es lo crítico y que no, para no desgastar esfuerzos y recursos sobre información que no merece la pena.

- Plataformas de captura y análisis de tráfico.

Los que me conocen, saben que este es uno de los temas que más me gusta. Todo lo que pasa o deja de pasar en nuestras infraestructuras de redes y sistemas, en algún momento circula por la red. Si somos capaces de entender estos flujos de tráfico, tenemos un gran punto a favor. Nuevamente debemos ser proactivos. No podemos implementar este tipo de herramientas o

plataformas "a toro pasado", es imprescindible tenerlas listas en las zonas estratégicas en las que deben operar y de ser posibles ajustar el concepto de "ruido de red" presentado hace unos años por Cisco y comentado ya en otras publicaciones nuestras. Si controlamos el tema de captura y análisis de tráfico, seguramente podamos tener patrones de conducta normales y anómalos previamente definidos y analizados. De hecho, ya venimos trabajado desde hace varios años con este concepto, almacenando y procesando esta información de forma tal que contamos en nuestras redes con bases de análisis historia de sus segmentos, servicios y plataformas, que nos permiten realizar comparativas durante cualquier tipo de análisis forense. Fijaros la importancia que esto tiene, a la hora de evaluar un comportamiento anómalo, cuando ya poseemos los patrones de tráfico históricos, filtros de captura y visualización que hemos implementado para llegar a esa árbol concreto del bosque de nuestra organización, cuando conocemos qué puertos, sockets y sesiones se establecen a diario, etc.

Este punto, es necesario dividirlo en tres partes. La primera es poco a poco ir montando una infraestructura de sondas y herramientas de captura de tráfico en nuestras redes, ajustando las mismas y aprendiendo su funcionamiento óptimo. La segunda es la recolección y determinación de la periodicidad adecuada para cada área, segmento o plataforma. Y la tercera que ya es la objetivos e máxima, es poder avanzar sobre esta implementación forma productiva como sistemas de detección y/o prevención de intrusiones.

Por supuesto que todas estas implementaciones, pensadas también en un futuro análisis forense, nos aporta un valor agregado muy importante.

- Herramientas de recuperación de información borrada.

El borrado no deseado de la información es una de las mayores preocupaciones de cualquier administrador de sistemas. Independientemente del punto de vista d ella seguridad, desde la visión forense, suele ser una de las actividades más frecuentes,

pues todo intruso que sepa lo que hace, sí o sí borrará sus huellas. La recuperación de las mismas nos ofrece una información valiosísima para comprender la secuencia de acciones que realizó. Muchas veces también, y cada vez con más frecuencia, se producen ataques con la única intención de causar daño borrando o criptografiando información de nuestro empresa.

En cualquiera de estos casos, la responsabilidad forense pasa por tratar de recuperar la información perdida. Al final de este capítulo nos detendremos en la herramientas más comunes para esta actividad, pero aquí deseábamos poner de manifiesto que es importante tomar las previsiones necesarias con las mismas, y por supuesto avanzar en su estudio, instalación y uso de las mismas antes que suceda un incidente o que tengamos que realizar un análisis forense.

- Redacción de un procedimiento sencillo y claro de actividades forenses.

  Este procedimiento, debe ser una guía prácticas de pasos a seguir y sobre todo de precauciones y medidas que no pueden descuidarse para evitar cualquier tipo de fallos en la legislación y el peritaje judicial. Tal cual hemos mencionado al principio del capítulo, la mejor referencia para la redacción del mismo la encontraremos en la norma **ISO/IEC 27037**:2012.

- Modelos predefinidos de formularios y reportes técnicos de análisis forense.

  Recordemos, que la fase 5 de la norma que acabamos de mencionar es la de "Reportes". Para que los mismos respondan a nuestro sistema de gestión documental, una muy buena práctica es tener plantillas y formatos modelo que contemplen los campos básicos que no deben ser dejados de lado y nos permitan darle una forma homogénea a todo el análisis.

- Formación del personal en gestión de incidentes.

Este tal vez sea el punto más importante, y en particular porque no aplica únicamente al personal involucrado específicamente en la actividad, sino que debe ser una preocupación de toda la organización, pues recordad que al suceder un incidente, cualquier acción apresurada y no practicada puede hacernos perder evidencias de mucho valor, por lo que todos los miembros de la organización deberían recibir capacitación sobre incidentes y posterior análisis y ser conscientes de la importancia de las acciones que puedan o no realizar, y por supuesto, conocer en detalle la cadena de escalado en estos temas.

Para esta "proactividad forense, la mejor herramienta para preparación forense bajo la filosofía open source, sin lugar a dudas es "**CAINE**" (Computer Aided INvestigate Environment).

Se trata de un sistema operativo completo Linux, bajo la distribución Ubuntu, que tiene embebido la totalidad de las herramientas necesarias para realizar una actividad forense con la mayor eficiencia.

La página Web de este desarrollo es:

https://www.caine-live.net

En la misma se encuentra toda la documentación detallada sobre esta poderosa herramienta.

En la actualidad su última versión es la 11 "Wormhole" y el responsable del proyecto es el italiano **Nanni Bassetti**.

No es la intención de este libro, presentar un curso de CAINE, pero sí invitaros a que la tengáis en cuenta, en particular como "proactividad forense", desde el punto de vista de su estudio, preparación, ejercitación y sobre todo configuraciones y ajustes sobre la arquitectura de nuestra organización, para que llegado el caso podamos aprovecharla al máximo.

Nuestra recomendación es que instaléis una máquina virtual con CAINE, la configuréis adecuadamente, en particular sobre sus conexiones de

red y el acceso a dispositivos físicos, y sobre la misma dediquéis todas las horas posibles a su estudio, y como acabamos de mencionar, la dejéis bien preparada y ajustada para que pueda ser empleada en tiempo real si fuera necesario desarrollar un análisis forense en nuestra organización.

Teniendo en cuenta que algunas de las herramientas que presentamos a continuación, ya están instaladas en CAINE y otras no, ponemos aquí abajo algunas sobre las que creemos es necesario conocer y saber emplear.

a. Herramientas específicas para análisis forense

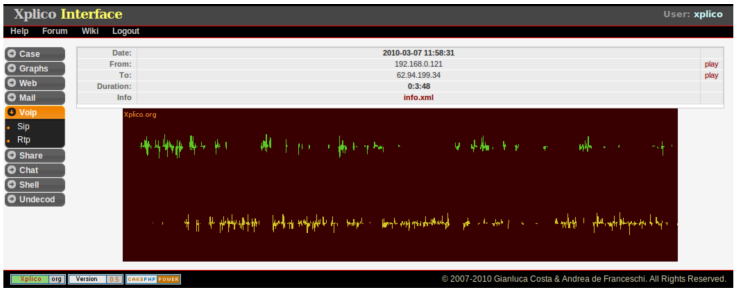
- The Sleuth Kit.

  Es un conjunto de herramientas open source para el análisis de imágenes de discos. Inicialmente desarrollada para plataformas UNIX, esta suite actualmente se encuentra disponible también para OS X y Windows. Además, TSK cuenta con una interfaz gráfica conocida como **Autopsy** que agrupa todas sus herramientas y plugins.

b. Herramientas de análisis de red

Las herramientas o comandos que se mencionan a continuación, son muy conocidas y son la base de cualquier persona que trabaje frecuentemente en redes. Durante un análisis forense, la posibilidad de hacer análisis de tráfico on-line u off-line, nos facilitará la comprensión de lo que circula por las redes.

- nmap
- tcpdump
- Wireshark
- Xplico



Interfaz gráfica de Xplico

c. Trabajo con discos

Tengamos en cuenta los conceptos anteriores, sobre la importancia de ser capaz de recuperar información borrada o inclusive poder

hacer búsquedas de rastros que hayan podido quedar almacenados. A continuación se presentan algunas de las herramientas y comandos más conocidos para operar sobre los medios de almacenamiento.

- Comando dd
- Dcdd3
- HDCLone
- Guymager
- Recuva
- DiskDrill
- Photorec

Logo

Logo HDClone

Recuva

Logo DiskDrill

d. Tratamiento de memoria

- Volatily
- Memoryze
- RedLine

e. Análisis de aplicaciones

- OllyDbg
- Radare2
- Process explorer

Logo OllyDbg

Logo Radare2

f. Detección de intrusiones.

- Snort
- Check Point Intrusion Prevention System
- Cisco Next Generation IPS
- McAfee Network Security Platform
- Se pueden considerar aquí los FWs NG de Palo Alto

g. Gestión de FWs.

- Algosec
- Tufin
- Firemon

h. Centralización y correlación de Logs (SIEM: Security Information and Event Management) del tipo.

- ArcSight de HP
- RSA Security Analytics
- Splunk (Puede discutirse si es o no un SIEM…)

i. Herramientas de control de acceso, tipo.

- ACS de Cisco
- Series SRC de Juniper
- NAKINA
- Access Control de Fortinet
- HPNA
- CITRIX

12. Procesos de ciberseguridad relacionados a Resiliencia.

Para comenzar este capítulo, en primer lugar recomendamos la lectura del capítulo 6. Ciberseguridad: La importancia de los procesos, del libro "**Ciberseguridad" (Una Estrategia Informático/Militar)** que puede descargarse gratuitamente de nuestra web: www.darFe.es.

Citando la introducción del mismo, se expone que:

> *Los procesos pueden parecer poco interesantes para alguien que desea dedicarse a Ciberseguridad, pero nuestra experiencia al respecto es que juegan un rol fundamental en toda organización de la Seguridad, pues son los que verdaderamente regulan "qué se puede y que no se puede hacer"; sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios, procederes, reacciones… cualquiera de estas palabras suenan a ¡Peligro! en alguien que se dedique a estos temas.*
>
> *A lo largo de estos últimos años, hemos tenido la posibilidad de auditar un importante número de redes y también a realizar el seguimiento y retesting de las mismas, lo que más nos llamó la atención es, justamente, que gracias a haber hecho un fuerte hincapié en estos procesos se ha manifestado un cambio radical en todas ellas.*

Como venimos haciendo a lo largo de todo el libro, una vez más iremos dando forma al tema tomando como punto de partida la norma **ISO/IEC 27001** de 2017, la cual establece:

> *7.5 Información documentada.*
>
> *7.5.1 Consideraciones generales:*
>
> *El sistema de gestión de la seguridad de la información de la organización debe incluir:*
>
> *a) la información documentada requerida por esta norma internacional;*
>
> *b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.*

7.5.2 Creación y actualización

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional se debe controlar para asegurarse que:

a) esté disponible y preparada para su uso, dónde y cuándo se necesite;

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluida la preservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión);

f) retención y disposición.

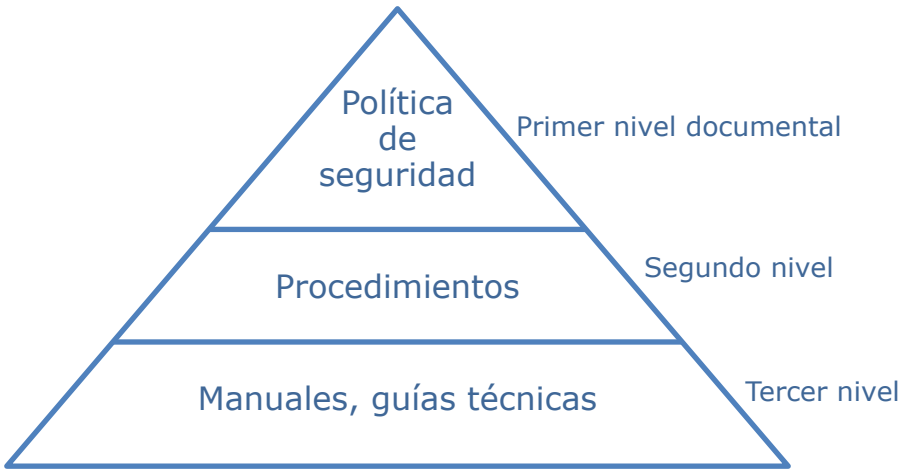
En su Anexo A establece los objetivos de control y controles de referencia, siendo el primero de ellos las Políticas para la seguridad de la información, estableciendo que:

Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Es decir, para que un SGSI funcione adecuadamente, debe contar con "Información documentada" sólida, lo que implica un ciclo de vida también

pero de la documentación. La misma parte de un "conjunto de políticas de seguridad", las cuáles marcan las líneas generales que la organización debe cumplir. Si siguiéramos analizando más en detalle la norma veríamos que impone de forma mandatoria un conjunto de documentos que están bastante referenciados de forma pública en Internet, una página web muy bien lograda al respecto es http://iso27000.es, en se puede encontrar un excelente resumen de los documentos obligatorios y no obligatorios de este estándar. Al tomar como punto de partida esta "Política de Seguridad", en la misma ya se debería hacer referencia a un segundo nivel de documentación, el cual por ejemplo podría estar compuesto por estos "procesos" o procedimientos que ya entran más en detalle en cada uno de esos aspectos y describen toda una serie de consideraciones que la organización deberá considerar. Por último, cuando ya se baja al nivel de tecnología, estos se desagregan a su vez como manuales o guías técnicas.

Como acabamos de presentar entonces, esta "Información documentada" que describe el estándar, debemos pensarla como una verdadera "**Jerarquía documental**" que al menos tiene que tener en cuenta tres niveles:



Cuando existe una estructura de documentación, y se plantea un ciclo de vida de la misma, tema estrictamente lógico, pues debe ser dinámica, ajustarse a los cambios tecnológicos, de la organización, a incrementos y variaciones de sistemas y redes, a nuevas medidas de seguridad, etc. Comienzan a plantearse una serie de interrogantes que también deben ser tenidos en cuenta: Su clasificación, quién la aprueba, cómo se sabe cuál es la última versión, quién puede o no acceder a la misma, quién está autorizado o no a hacer cambios, cómo llego hasta ella, quién es el responsable, propietario, usuario de ella, etc.

En la actualidad, es muy difícil mantener viva una estructura documental, sin un adecuado sistema o proceso de gestión documental. En el mercado existe una gran cantidad de estas plataformas, tanto de pago como de open source, una muy buena elección como Open source es

Alfresco Community Edition, que es la versión software libre, con licencia **LGPL** (GNU Lesser General Public License) y estándares abiertos. Puede descargarse en: https://www.alfresco.com/

Independientemente de la tecnología que decidamos usar, es necesario comprender bien de qué se trata un gestor documental, para ello recurramos una vez más a "Wikipedia" que lo define en el siguiente enlace: https://es.wikipedia.org/wiki/Gestión_documental

Según Wikipedia:

> *Procesos de la Gestión DocumentalUn sistema de gestión documental por lo general se refiere a las siguientes áreas: Almacenamiento, recuperación, clasificación, seguridad, custodia, distribución, creación, autenticación.*

Almacenamiento	¿Dónde guardaremos nuestros documentos? ¿Cuánto podemos pagar para almacenarlos?
Recuperación	¿Cómo puede la gente encontrar documentos necesarios? ¿Cuánto tiempo se puede pasar buscándolo? ¿Qué opciones tecnológicas están disponibles para la recuperación?
Clasificación	¿Cómo organizamos nuestros documentos? ¿Cómo aseguramos que los documentos estén archivados siguiendo el sistema más apropiado?
Seguridad	¿Cómo evitamos la pérdida de documentos, evitar la violación de la información o la destrucción no deseada de documentos? ¿Cómo mantenemos la información crítica oculta a quién no debiera tener acceso a ella?
Custodia	¿Cómo decidimos qué documentos conservar? ¿Por cuánto tiempo deben ser guardados? ¿Cómo procedemos a su eliminación (expurgo de documentos)?
Distribución	¿Cómo distribuimos documentos a la gente que la necesita? ¿Cuánto podemos tardar para distribuir los documentos?
Workflow	¿Si los documentos necesitan pasar a partir de una persona a otra, cuáles son las reglas para el flujo de estos documentos?
Creación	¿Si más de una persona está implicada en creación o modificación de un documento, cómo se podrá colaborar en esas tareas?

Autenticación	¿Cómo proporcionamos los requisitos necesarios para la validación legal al gobierno y a la industria privada acerca de la originalidad de los documentos y cumplimos sus estándares para la autentificación?

En esta introducción se ha tratado de poner de manifiesto la importancia de contar con un buen sistema de gestión documental y organizar todos los documentos bajo una jerarquía que permita identificar el grado de detalle de cada uno de ellos. Se recomienda que esta actividad sea llevada a cabo con máxima consciencia, pues tal cual lo indica el estándar ISO 27001 es uno de los pilares básicos para mantener vivo un SGSI.

Sobre el tema de procedimientos, en España, en el mes de enero de 2010 se publicaron el **RD 03/2010 "Esquema Nacional de Seguridad"** (**ENS**) y el **RD 04/2010 "Esquema Nacional de Interoperabilidad"**. En esa época estaba dirigido eminentemente a las Administraciones Públicas (AAPP) españolas, en la actualidad se aplica en muchas empresas privadas y hasta existe una certificación sobre el ENS, pues como es lógico, las AAPP exigen un nivel de seguridad equivalente a toda empresa que quiera trabajar con ellas, lo que ha convertido a estas en un verdadero referente español en seguridad y tal cual lo expresé siempre, reconozco que es un excelente marco de referencia.

Ese año, por si os interesa, escribí un artículo al respecto: **Esquema Nacional de Seguridad, se lanzó la "cuenta atrás"**. Se puede descargar gratuitamente en:

https://darfe.es/es/nuevas-descargas/category/4-tec

Como acabo de mencionar, este marco se fue imponiendo en las empresas españolas y desde sus inicios se fue alineando con la familia I**SO 27000**, tanto es así que cualquier empresa que esté alineada con ISO 27000, le será muy sencillo la certificación en el ENS. También en el año 2010 escribí otro artículo en relación a ambas normas: **"Esquema Nacional de Seguridad e ISO 27001 ¿Cómo implantar ambos en mi empresa?**", por si os interesa está en:

https://darfe.es/es/nuevas-descargas/category/4-tec

Todo esto viene a relación en que los aspectos normativos del ENS fueron delegados al **Centro Cripotológico Nacional** de España (**CCN**), que es un organismo de reconocido prestigio nacional e internacional dependiente del Centro Nacional de Inteligencia (**CNI**).

Dentro de la página Web del CCN podéis encontrar información de muy buena calidad:

https://www.ccn.cni.es/index.php/es/

A su vez, una de las responsabilidades del CCN es el **CERT** (Computer Emergency Response Team), que en España, se lo conoce como "CCN-CERT". Me encanta el lema que figura en su página de enlace" "*Defensa del ciberespacio español*":

Su web es: https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es.

En la misma, ahora sí voy al tema en concreto, figuran todas las guías de seguridad del ENS, las cuáles son de gratuita descarga y no me canso de recomendar por su nivel de excelencia. No pueden ser dejadas de lado por cualquier responsable de ciberseguridad. Se las reconoce como la "**familia 800**" y todas ellas son una referencia de máximo nivel para organizar nuestros procedimientos de seguridad, podéis descargarlas en:

https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

Estas guías establecen unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. El listado completo de las mismas se encuentra en:

https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

12.1. Gobierno de la Ciberseguridad.

Comenzando una vez más por el estándar **ISO/IEC-27001**, el mismo, en el punto 5.3 "Roles, responsabilidades y autoridades en la organización", establece que:

> *"La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.*
>
> *La alta dirección debe asignar la responsabilidad y autoridad para:*
> *a) asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional; e*
> *b) informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información".*

Continúa esta norma con otros puntos que nos interesan. No podemos entrar en todo el detalle que quisiéramos sobre cada uno de ellos, pues estaríamos desarrollando gran parte del estándar y no es correcto hacerlo, por lo que nos limitaremos a citarlos para dar pie a la explicación posterior, sobre qué aspectos fundamentales debería considerar al menos este procedimiento.

Los otros puntos que nos interesan tener en cuenta son

> *6 Planificación*
> *a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;*
> *b) prevenir o reducir efectos indeseados; y*
> *c) lograr la mejora continua.*
>
> *6.2 Objetivos de seguridad de la información y planificación para su consecución*
>
> *La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.*
>
> *8 Operación*

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

9.3 Revisión por la dirección

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

10 Mejora (Varios aspectos referidos a mejora continua)

Yendo a su anexo, debemos tener en cuenta también los siguientes controles:

A.5 Políticas de seguridad de la información
A.5.1 Directrices de gestión de la seguridad de la información
A.6 Organización de la seguridad de la información
A.18.2 Revisiones de la seguridad de la información

Si tenemos acceso a la norma, podremos desarrollar cada uno de estos temas propuestos, en caso contrario, a continuación presentamos una propuesta de cómo podemos organizar este documento y cuáles son los puntos clave a desarrollar.

Objeto

Este primer proceso, recordemos que se desencadena de la "política de seguridad" de nuestra empresa, por lo que debe responder a este lineamiento general que ya se ha establecido.

Sería una muy buena medida, que el "Gobierno de la Seguridad" haya sido planteado desde la misma política, con la finalidad de dejar clara la importancia de la seguridad dentro de la organización y que se ponga de manifiesto el compromiso de la dirección desde la raíz documental.

Una vez dejado claro este punto de partida, el objeto concreto de este documento será el de definir los controles mínimos que se deberán implantar en la organización y sobre qué ámbito aplicará cada uno de ellos o de forma global.

Organigrama de Gobierno de la seguridad

Este organigrama por supuesto dependerá de la magnitud de la empresa, no pudiendo establecer una medida concreta del mismo, pero a los efectos de este libro dejaremos las pautas a tener en cuenta para una gran empresa, con la intención que cada lector pueda tomar esta idea como referencia y adecuarla a su organización, creemos que siempre es más sencillo acotar el problema que intentar escalar sobre bases o referencias desconocidas.

El máximo órgano de una gran empresa debería ser el "**Comité de Seguridad**" el cual puede estar constituido por diferentes perfiles, pero siempre teniendo presente que deberá poder adoptar decisiones críticas, por lo que es conveniente que formen parte del mismo miembros de la alta dirección, y se integren también personal jerárquico de las áreas clave (Finanzas, Operaciones de red y TI, RRHH, Legal, Auditoría y por supuesto Seguridad).

El área técnica de este Comité puede formar parte o no del mismo, o puede ser un Subcomité asesor, este segundo nivel más técnico debería contar con áreas o especialistas en: Seguridad de redes y TI, Ciberinteligencia, Ciberamenazas, Investigación y prevención del fraude, Cumplimiento legal, y control y manejo de medios de difusión.

Por último, debería existir un tercer nivel dentro de este organigrama, en el cual se encuentran los especialistas de la operación de las seguridad. En este nivel ya se busca el perfil

específico de un técnico programador, especialistas en hacking ético, expertos en firewalls, routers, proxies, sistemas operativos, bases de datos, herramientas de seguridad, IDSs, IPSs, criptografía, túneles, protocolos seguros, consolas, certificaciones de seguridad, etc.

Funciones

La descripción de las funciones de cada uno de ellos debe dejar reflejada con total claridad sus responsabilidades y obligaciones y en particular, tal cual establece la norma ISO/IEC 27001 "antes", "durante" y "después" de sus contratos.

Un aspecto que NO se debe pasar por alto son las penalizaciones y medidas disciplinarias que aplican a las funciones que se desempeñen.

Jamás hay que olvidarse que lo que no está escrito e informado puede ocasionar la invalidez de cualquier acto jurídico.

Metodología de gestión de la seguridad

El aspecto más importante de la gestión de la seguridad es la consciencia de "**ciclo de vida**", es decir, mantenerse siempre en la idea que lo que no se actualiza NO sirve. Tomando este lema como factor clave del diseño e implantación de un SGSI es que en cada uno de sus pasos y acciones, tendremos presente de qué forma se mantiene vivo el mismo. Ya hemos desarrollado todos los pasos que nos permiten lanzar un SGSI, en el último capítulo desarrollamos las métricas, ahora estamos desarrollando como se gobierna la seguridad, por lo que en este documento deberemos dejar clara la forma de cerrar el ciclo. La gestión de la seguridad es el eslabón final que nos permite desarrollar el "Act" de este ciclo PDCA. Veremos a continuación que en este documento se debe considerar la planificación y el seguimiento, y finalmente la mejora continua. Con la redacción de las acciones concretas de cada uno de ellos en este

procedimiento estamos definiendo justamente este metodología que aplicará a nuestro SGSI.

Planificación de la seguridad

Hemos puesto de manifiesto reiteradas veces que la seguridad no puede ser considerada como algo estático, es un ciclo de vida que exigirá permanentemente transformaciones e incorporación de nuevas medidas, recursos e iniciativas para su mejora continua.

Una medida muy acertada es la elaboración de un "**Plan director de Seguridad**" que determine las pautas generales que marcarán el rumbo de este proceso de planificación.

Nada peor que la improvisación en las decisiones de seguridad de una organización. Una muy buena práctica en la dirección de redes y TI de una empresa es contar con tres áreas bien diferenciadas: planificación, ingeniería y operación. En este apartado nos interesa hacer referencia a la primera de ellas que será la responsable del análisis de mercado y el diseño de este plan, en nuestro caso en lo que a ciberseguridad se refiere, luego será ingeniería quien defina el proceso de entrada en producción y una ve implantado caerá en manos de operación para el día a día.

Seguimiento

El "Check" de ese ciclo PDCA es la clave de este punto. La monitorización regular y los reportes de evolución son la actividad a desarrollar para evaluar lo diferentes estados por lo que va pasando este ciclo de vida. Este punto es una responsabilidad que debe ser bien definida entre seguridad y auditoría para que queden claros sus responsabilidades.

Los reportes que se generen, deberán ser tratados periódicamente por el comité de seguridad para que adopte las

decisiones oportunas acerca de los desvíos o el desempeño de la organización, respecto al SGSI. Este tipo de reportes deberá presentar:

- Conclusiones
- Propuestas
- Recomendaciones

Que darán soporte al cuadro de mando global.

Como se irá desarrollando en este libro, uno de los factores clave para esta actividad de seguimiento es una buena definición y empleo de los KPI que ya hemos presentado. Una adecuada definición y mantenimiento de este tipo de métricas e indicadores será el factor de éxito.

Plan de auditorías

Como se acaba de mencionar, los reportes sobre el seguimiento de los niveles de seguridad son una responsabilidad que debe quedar claramente establecida entra seguridad y auditoría. En el caso de auditoría, deberá verse reflejado también a través de un plan de auditoría que suele ser anual.

Este plan se dividirá en auditorías internas y externas, en el caso que la organización cuente con un área específica de auditoría propia, en caso contrario deberá adoptar las decisiones necesarias para lograr un equilibrio lo más coherente posible entre ser "juez y parte" dentro de áreas o personas concretas en la empresa para que puedan llevar a cabo este tipo de revisiones, aunque es necesario dejar claro que esto no es lo ideal. Cuando no se cuenta con un área de auditoría interna, para los temas relevantes lo correcto e contratarlas a un tercero, por medio de la realización de auditorías externas, y solo en los casos muy puntuales recurrir a personal propio, siendo conscientes que el mismo siempre tendrá algún tipo de dependencia o compromiso con el área auditada, cosa que no sucede (o no debería) si la organización cuenta con un área de auditoría interna.

El punto de partida o los "inputs" de una plan de auditoría de seguridad, debería ser tomado del análisis de riesgo y el curso de acción elegido por la dirección que hemos presentado en los capítulos anteriores, pues fue allí donde se definieron las acciones a adoptar para mitigar los riesgos identificados, es decir que se puso de manifiesto que habrá hitos de control intermedios y estados de avance sobre los riesgos a los que están expuestos los activos críticos. Este tipo de revisiones independientes del área de seguridad, son las que necesita la dirección para estar segura, o no, de cómo va evolucionando ese curso de acción elegido y si sus decisiones y la implantación de las mismas están en el camino adecuado. Sobre esta base es como se debe diseñar el plan de auditoría y sus reportes deberían intentar mantener un punto e vista homogéneo con el aspecto en el que se presentaron los diferentes cursos de acción (*recordad, o volved, a la última imagen presentada al final del capítulo 9*).

Por último, dentro del plan de auditoría, es fundamental incluir también todos los aspectos de seguridad que deben ser controlados sobre nuevos proyectos estratégicos a los que la organización se haya volcado y no formen parte aún del análisis de riesgo, pues aún se trataban de proyectos. En el proceso de implantación o entrada en producción de los mismos es fundamental que el área de auditoría forme parte, estableciendo los hitos de control necesarios en este mismo plan.

Mejora de la seguridad

La mejora de la seguridad se refleja en primer lugar en los "Planes de acciones correctivas". Cuando se generan reportes en los que se evidencias desvíos de lo planificado, el proceder adecuado es que, al ser tratados por el Comité de seguridad, el mismo los presente ante el área responsable, se analice el hallazgo para verificar que es correcto, se pongan de acuerdo con las propuestas y recomendaciones y luego se defina un "Plan de acciones correctivas" donde las medidas, responsables y

plazos deben quedar claramente establecidos. El seguimiento y "re testing" de las acciones correctivas quedará en manos de quien generó el reporte (seguridad y/o auditoría).

El segundo factor clave en las acciones de mejora, en todo SGSI es cuando se han alcanzado los umbrales planificados para cada KPI en el ciclo de vida que se está ejecutando. Ampliemos este tema con detalle.

Pongamos el caso más claro que es cuando una empresa inicia un proceso de certificación en el estándar ISO/IEC 27001. En esa primera certificación, y en las sucesivas, jamás se le exigirá la perfección, pues la misma, recordemos que es inalcanzable (*y enemiga de lo bueno…*). Se le irá requiriendo un umbral inicial mínimo a cumplir y luego, ciclo a ciclo, una escalada secuencial y lógica que demuestre que está haciendo un esfuerzo, justamente de "mejora continua" en su nivel de seguridad. De esto se trata la idea de SGSI. Para cumplir con esto, es necesario ese análisis de riesgo que desarrollamos al principio, la selección de un curso de acción y un plan de implantación del SGSI. Este proceso se va midiendo a través de esos KPI y métricas que hemos desarrollado también en los capítulos anteriores. Cada uno de ellos, como es lógico, no necesariamente será definido una escala de crecimiento de cero a cien en un solo ciclo de vida, pues es muy probable que no haya presupuesto que lo aguante. Lo más natural es, tal cual hemos hecho desde el principio, comenzar con "trazo grueso" como nos aconsejaba MAGERIT y proponernos, por ejemplo centrar todos nuestros esfuerzos sobre los activos críticos (como también presentamos en nuestro análisis de resiliencia). Si seguimos con este ejemplo, y la dirección seleccionó un curso de acción que no sea el de máxima (o inclusive si hubiera elegido ese mismo), en nuestro proceso de imantación iremos definiendo justamente estos KPI o métricas que nos permitirán ir evaluando el estado de ejecución. En el caso concreto que hemos presentado en los capítulos 7, 8 y 9 se pone de manifiesto concretamente que nuestros KPI no apuntaban a un 100 % de completamiento, nuestro análisis y planes de acción justamente era para un período de dos años. Al finalizar esta

etapa, será necesario verificar el grado de cumplimiento de los mismos que se ha alcanzado y proyectar nuevos parámetros, métricas y umbrales de medición para que el siguiente período puede nuevamente demostrar un esfuerzo de mejora y que el mismo sea debidamente cuantifícale y sobre todo medible. En grandes líneas esta es la clave de la "Mejora continua".

12.2. Plan de recuperación de desastres (DRP: Disaster Recovery Plan).

En este capítulo, hemos preferido tratar en detalle el tema de DRP, en el siguiente desarrollaremos el "Plan de Continuidad de Negocio", más conocido por sus siglas en inglés **BCP** (Business Continuity Plan). En nuestra opinión, la diferencia más importante entre el DRP y el BCP es que el primero de ellos es más reactivo y el segundo proactivo, también es cierto que el DRP está incluido en un BCP, es una parte del mismo.

En nuestra experiencia, el DRP es algo que siempre se encuentra en las organizaciones y con un importante grado de implantación, en cambio el BCP suele encontrarse más en estado teórico que en su parte práctica. Es probable que sea por una cuestión de costes y esfuerzo, por esa razón, basados eminentemente en nuestra experiencia, pero sobre todo para que podamos abordar el tema de forma práctica y efectiva, es que preferimos comenzar por aquí, y teniendo en cuenta que nuestro objetivo son redes y sistemas resilientes, un DRP no puede dejar de existir bajo ningún punto de vista.

Según "Wikipedia".

(https://es.wikipedia.org/wiki/Plan_de_recuperación_ante_desastres)

> *Un plan de recuperación ante desastres (del inglés Disaster Recovery Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, el propósito es la protección de datos.*

Hemos puesto esta definición de Wikipedia en particular, porque el "personal clave" parece que es uno de los grandes olvidados de un DRP. Siempre pongo de manifiesto un caso real que sucedió en un entorno muy próximo donde yo trabajaba aquí en Madrid, en el que el personal del NOC, solía ir a comer siempre al mismo sitio, quedaba una persona de guardia y el

resto hacía su parada diaria del almuerzo todos juntos. Un día en el restaurante que fueron, hubo un brote de salmonela y cayeron todos los del NOC (menos uno de guardia), fue un hecho que aunque hoy parezca cómico, causó estragos en la empresa y estuvieron un mes completo intentando paliar la operación diaria de un NOC importante con gente no capacitada. Esto se incluyó en el DRP de la empresa y el NOC continuó su trabajo comiendo por turnos el resto de su vida. Aquí se pone de manifiesto claramente el carácter reactivo de un DRP.

Ya hemos hablado en el capítulo 8 de los conceptos de **RPO** y **RTO** como parte de nuestra "Matriz de Resiliencia", justamente estos parámetros son dos cálculos indispensables en la recuperación de cualquier desastre, pues para los activos críticos, ya se trató, que cuanto más precisos seamos acerca de qué punto y en que tiempo necesito volver a tenerlos en servicio, sobre estos márgenes es donde debo calcular las medidas adecuadas para hacerlo. No es lo mismo tener que recuperar una base de datos con un RTO y/o RPO de minutos, cosa que sucede muy a menudo, por ejemplo en la facturación de una gran empresa telefónica que está cursando cientos de miles de llamadas por minuto y la pérdida de un solo minuto de facturación probablemente sea más onerosa que el valor de la base de datos completa con su hardware y software incluidos, que una mucho más estática como puede ser de perfiles de usuarios que con ser diaria es más que suficiente o una de nóminas que puede llegar a ser mensual. La planificación, esfuerzo y recursos de cada una de ellas serán sustancialmente diferentes.

A su vez un adecuado cálculo y mantenimiento del ciclo de vida de estos parámetros para cada activo crítico, nos hará optimizar presupuestos y recursos, dando como resultado una capacidad de resiliencia mucho mejor.

Un documento que queremos hacer referencia del **NIST** (National Institute of Standards and Technology) es "**Special Publication 800-184 - Guide for Cybersecurity Event Recovery**" de diciembre de 2016, que puede descargarse en:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

El propósito de este documento es apoyar a las organizaciones en tecnologías para mejorar sus planes, procesos y procedimientos de recuperación de ciberincidentes, con el objetivo de reanudar las operaciones normales más rápidamente.

El documento describe la necesidad de una planificación de recuperación efectiva antes de un evento cibernético, proporciona información sobre cómo mejorar la resiliencia empresarial, los procesos y procedimientos de recuperación, las comunicaciones de recuperación y el intercambio de información. Hace referencia también a tareas para lograr la mejora continua de los procesos de recuperación y la postura de seguridad de la organización. Pone bastante hincapié en la necesidad de validar las capacidades de recuperación utilizando una variedad de técnicas, incluida la solicitud de retroalimentación del personal sobre planes, políticas y procedimientos de recuperación, y la realización periódica de ejercicios y pruebas que aborden la recuperación del mundo real. Como parte práctica brinda ejemplos de métricas de recuperación que pueden ayudar a las organizaciones a medir y monitorizar su rendimiento de recuperación a lo largo del tiempo.

Propone fases tácticas y estratégicas con escenarios de recuperación de evento cibernéticos de violación de datos.

Además de identificar posibles mejoras en las capacidades de recuperación a través de revisiones por parte del personal y pruebas y ejercicios periódicos, las organizaciones también deben identificar mejoras de las lecciones aprendidas durante las acciones reales de recuperación de eventos cibernéticos. Estas lecciones aprendidas ayudan a impulsar mejoras no solo en la recuperación en sí, sino también en las operaciones de seguridad, políticas, etc. de la organización.

Esta norma, presenta en la **Figura 3-1** el enfoque principal del documento que es la función recuperar con mecanismos de retroalimentación continua.

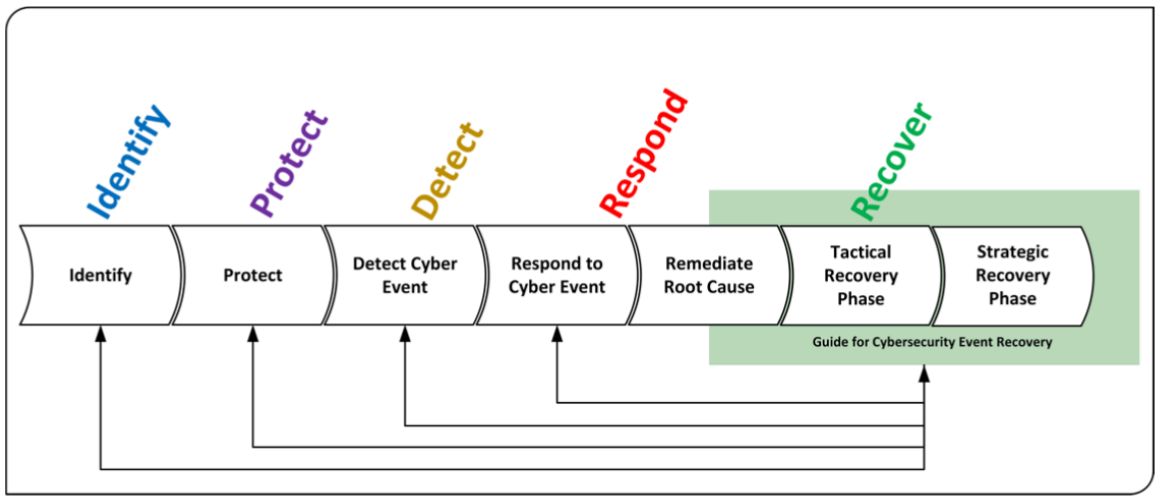
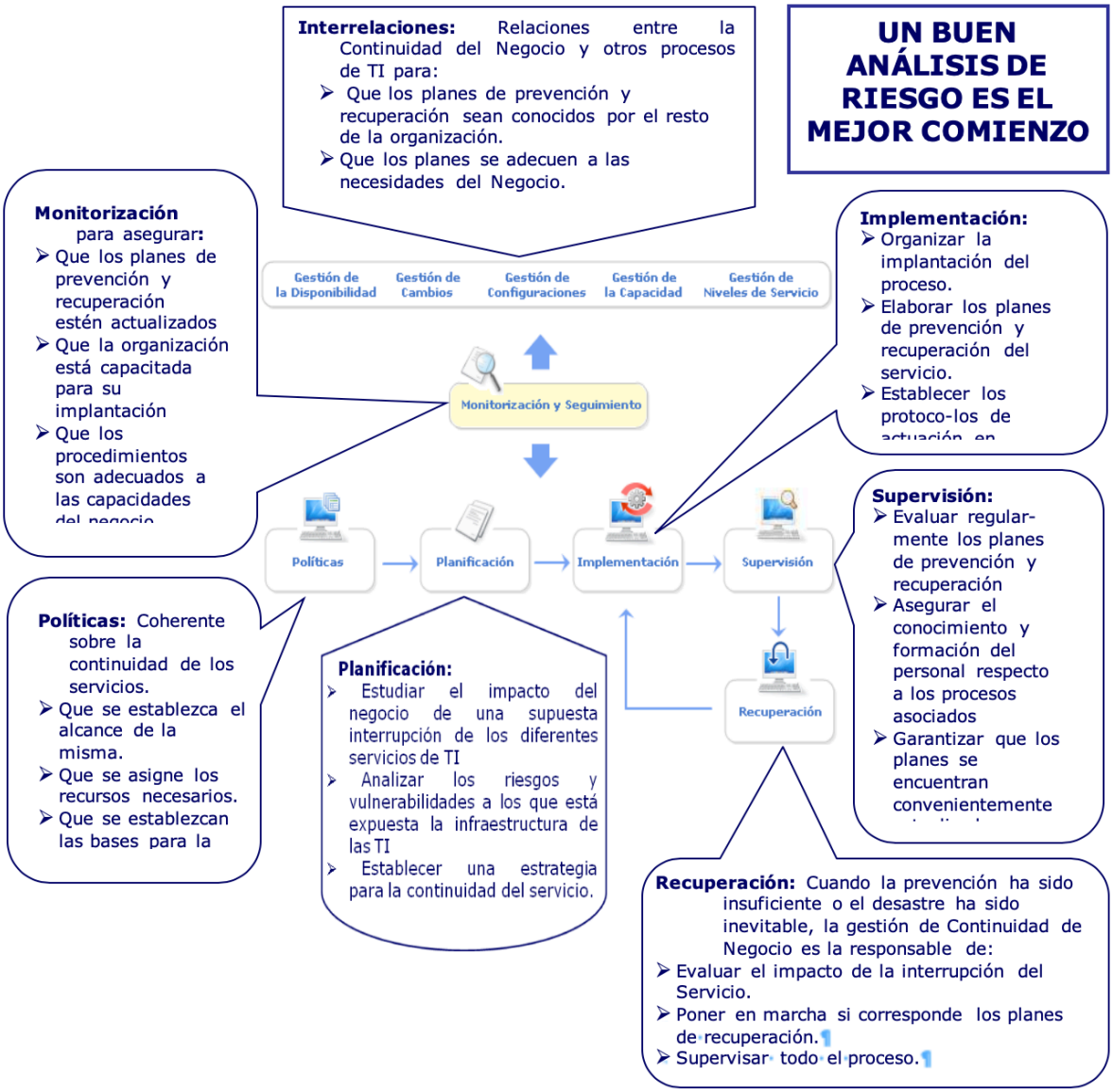


Figure 3-1: NIST SP 800-184 Guide for Cybersecurity Event Recovery Relationship with the NIST CSF

Una parte de este documento que nos parece especial es su **APÉNDICE A** que presenta un checklist de acciones para recuperación que merece la pena ser tenido en cuenta y aconsejamos su detallada lectura.

En mi anterior libro "**Seguridad por Niveles**", que puede descargarse gratuitamente de la web: www.darfe.es, en la sección "Nuevas Descargas", se presenta el tema completo del PCN en la **sección 8.7**, pero aquí desearía remarcar la importancia que en el mismo se hace sobre el "Plan de escalada".

Uno de los aspectos importantes de un DRP es el "Plan de escalada", que también debe formar parte de los procesos de la organización, si consideramos al DRP como un proceso más de gestión integrado dentro del SGSI, entonces pasa a formar parte del "Ciclo de vida de la seguridad", para ello lo debemos presentar como otro proceso más que considere al menos los siguientes pasos:



Un desastre para un sistema informático no es sólo el de las Torres Gemelas. Si un servidor de nuestra organización, sufrió una interrupción y se re inició, lo más probable es que no sea más que una mera "Incidencia", ahora, si nuestro servidor de "Comercio electrónico" se cae y al minuto no lo logramos levantar, ni a la hora, ni al día siguiente, esto empieza a preocupar a la empresa pues dejó de vender "On line" y eso toma el rostro de un "desastre". Este ejemplo concreto nos tocó vivir con una importante y muy conocida empresa de telefonía española (salió en todos los medios de comunicación) cuando se cayó durante casi dos días uno de los nodos principales de conmutación, y por supuesto todos los usuarios conectados al mismo "No hablaban, ni podía conectarse a Internet", este tipo de fallos son

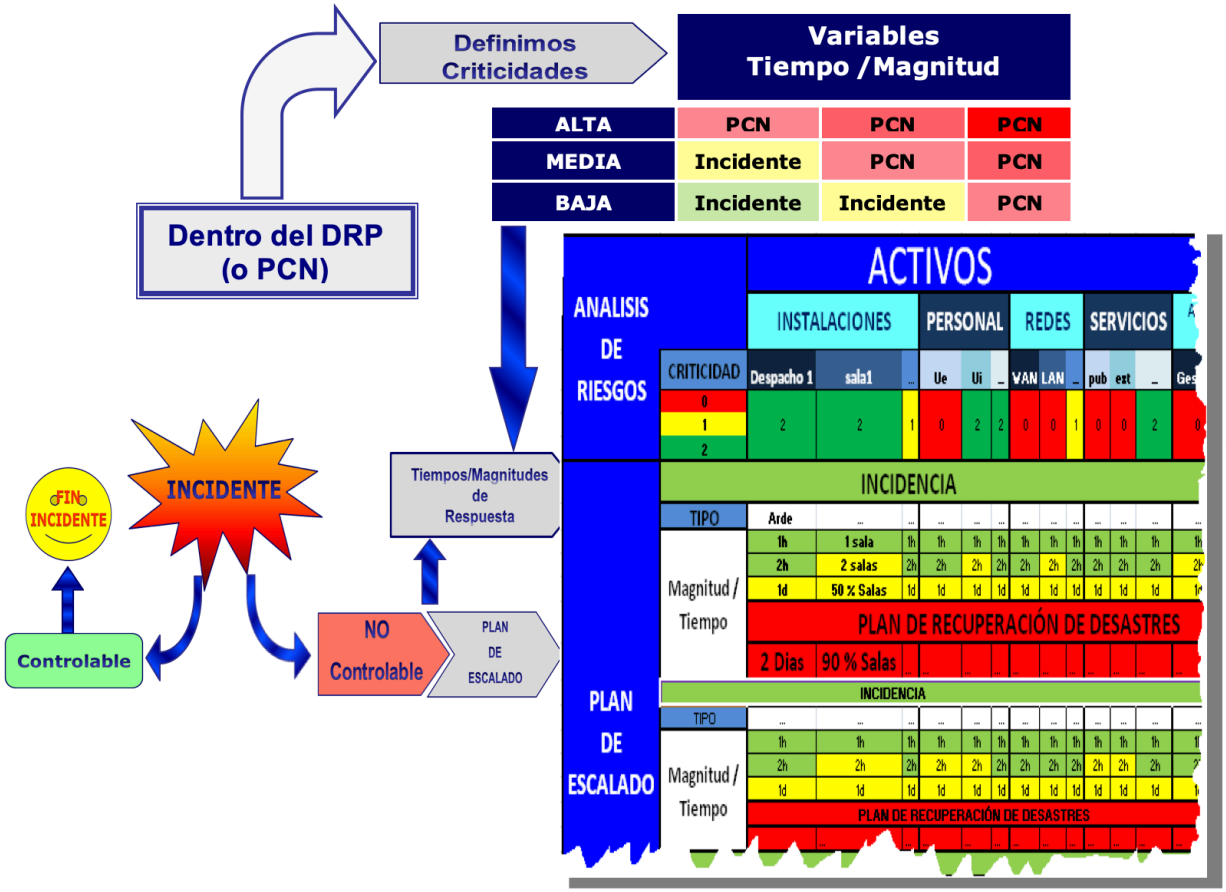
mucho más frecuentes de lo que la gente supone, pero duran instantes, lo feo es cuando comienzan a pasar los segundos sin facturación, toca bolsillos muy altos y esto empieza a ser grave e imperdonable (el vil dinero…).

A un desastre se llega por dos caminos:

- Inmediato.
- Escalada de incidentes leves.

Lo que intentamos transmitir es que un incidente menor, puede ir creciendo en su complejidad, desencadenar en un desastre y el PCN se puede llegar a activarse porque se prendió fuego el edificio, o también por una suma de desperfectos que simple vista pueden parecer inofensivos, pero que en conjunto pasan a ser "Letales". Siempre que hemos desarrollado este aspecto, tanto en teoría como en la práctica insistimos en la elaboración de lo que denominamos "Plan de escalada".

El Plan de escalada, reiteramos, es un proceso fundamental. Una forma de elaboración es definir cuáles pueden ser los escenarios en los que ocurren o pueden ocurrir incidencias. Si nuestros sistemas llevan tiempo en producción este es un dato estadístico muy conocido; luego evaluar diferentes valores de tiempo y recursos que de producirse harían escalar estas incidencias. Debemos tener en cuenta que como parte de un SGSI (u hoy en día cualquier infraestructura de seguridad) ya tenemos valores, métricas e indicadores, y si evaluamos correctamente nuestro Plan de escalada, contaremos con valores de "Umbrales" o KPI que serán los que desencadenan en un DRP y hasta puede que activen el PCN, todo esto se puede incorporar como un proceso más que responda a la siguiente lógica:



Acabamos de presentar cómo se puede llegar a un desastre, pero también hay otros conceptos que debemos considerar, por ejemplo:

- Duración: corta, mediana o larga.
- Origen:
  - Natural: Inundaciones, terremotos, tsunamis, volcanes, huracanes, tornados, inundaciones, nevadas, congelamiento, etc.
  - Inducido (voluntario o no): Incendios, robos, fraudes, terrorismo, delitos varios.

Si analizamos el DRP desde un enfoque normativo, el verdadero punto de partida puede ser la norma **ISO/IEC 24762:2008** "Information technology — Security techniques — **Guidelines for information and communications technology disaster recovery services**".

Esta norma se publica en 2008 y, si bien ha sido anulada en 2014 (pues gran parte de ella, como se verá en el capítulo siguiente, queda embebida en la **ISO 27031**), hay aspectos claves y específicos de un DRP que desearíamos poner de manifiesto.

Esta norma habla sobre el DRP desde un punto de vista interno y también en los casos en que se externalice el servicio, y este es un tema clave, pues es una realidad muy frecuente hoy en día. En los casos de contratación del servicio de recuperación de desastres, existen un sinnúmero de cláusulas o **SLA**s (Service Level Agreement - acuerdo de nivel de servicio) que son fundamentales a considerar, pues justamente entran en vigor al ocurrir este tipo de incidentes críticos y es el momento en el cual el servicio contratado NO puede fallar. Las medidas a tener en cuenta en los casos de subcontratación las hemos considerado de primer orden, pues hemos visto en reiteradas oportunidades contratos que no se encontraban debidamente "blindados" y a la hora de aplicarlos, cuando las cuantías del daño son altas, aparecen las "zonas grises" que dan pie a evadir responsabilidades o no cumplir con los tiempos y/o recursos necesarios en una respuesta óptima.

Este aspecto de la norma creemos que es de vital interés para el lector. Recomendamos la lectura del punto:

"5.11 Business continuity planning for ICT DR service providers" y con más detalle el "7 Outsourced service provider’s capability"

Siguiendo con esta norma, el punto "6 ICT disaster recovery facilities" centra su atención en las ubicaciones físicas y las características que deben ser tenidas en cuenta en las mismas. Este tipo de detalles son bien conocidos en el ámbito de las TICs (peligros naturales, cambios climáticos, peligros industriales y comerciales, accesibilidad, rutas de acceso, locales compartidos, etc.) pero lo importante de la norma es que los presenta de forma completa y en un orden que facilita su planificación, diseño y organización para que no quede nada de ello librado al azar. Completa este punto con los controles de acceso, el personal de seguridad, las diferentes zonas seguras, el trabajo fuera de horario, los tests, las autorizaciones y el personal de staff y no staff. Un aspecto que también es de especial interés en este punto, es el concepto de **EOC** (Emergency Operations Center) que difiere en muchos aspectos de los conocidos **NOC** (Network Operations Center) y **SOC** (Security Operations Center). Este punto 6 es un desarrollo

muy completo de esta norma (tal vez el que más) y que echamos en falta en los nuevos estándares.

Los dos puntos de contenido final de la norma son "8 Selection of recovery sites" y el infaltable "9 Continuous Improvement".

Por último es interesante también el Anexo A, en que en su "Table A.1 — Correspondence between ISO/IEC 27002:2005 and this International Standard" como su título lo indica, nos permite verificar el cumplimiento de cada uno de estos puntos si nuestra organización está implantando un SGSI siguiendo la propuesta de la familia ISO 27k.

12.3. Plan de Continuidad de Negocio.

El tema de BCP ya lo hemos desarrollado en el punto: 8.7. Plan de Continuidad de Negocio (PCN), del libro "**Seguridad por Niveles**" (que puedes descargar gratuitamente en: www.darFe.es), gran parte del tema ha sido desarrollado en ese libro, pero teniendo en cuenta que fue publicado en el año 2011, a continuación se presentarán temas de actualización sobre el tema.

Según Wikipedia:

https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio

> *Un plan de continuidad del negocio (o sus siglas en inglés BCP, por Business Continuity Plan) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.*

Como siempre solemos hacer, analicemos el estado actual de la normativa internacional sobre el tema.

La norma **ISO 22301-2105** "**Sistema de Gestión de Continuidad de Negocio**", es la norma certificable sobre BCP. Al igual que la **ISO 27001**, también define los conceptos básicos para administrar y desarrollar el BCP. Especifica la estructura y requerimientos para la implementación y mantenimiento de un "Business Continuity Management System (**BCMS**).

Un BCMS enfatiza sobre la importancia de:

- comprender las necesidades de la organización y la necesidad de establecer políticas y objetivos de continuidad del negocio.
- operar y mantener procesos, capacidades y estructuras de respuesta para garantizar que la organización sobreviva a las interrupciones.
- monitorizar y revisar el desempeño y la efectividad del BCMS;

- mejora continua basada en medidas cualitativas y cuantitativas.

Cuando se analiza una norma certificable, como en este caso la **ISO 22301**, es importante considerar los aspectos que la misma define como "**mandatorios**", pues ellos son los que justamente tienen que ser cumplidos con máximo detalle a la hora de solicitar su certificación a la empresa auditora externa. Más allá de tener planificado, o no, este tipo de certificaciones, también es una buena práctica considerarlos como una referencia a la hora de organizar nuestro BCMS, por lo que centremos nuestra atención unas líneas sobre estos.

Las normas ISO en sus "introducciones", en general, siempre hacen referencia a este tipo de aspectos, en el caso de este estándar, en el punto: 0.5 "Contents of this document" (contenidos de este documento) establece que:

> *"In this document, the following verbal forms are used:*
>
> *a) '**shall**' indicates a requirement;*
>
> *b) 'should' indicates a recommendation;*
>
> *c) 'may' indicates a permission;*
>
> *d) 'can' indicates a possibility or a capability."*

En español, esto significa:

> En este documento, se utilizan las siguientes formas verbales:
>
> a) "**deberá**" indica un requisito;
>
> b) "debería" indica una recomendación;
>
> c) "debe" indica un permiso;
>
> d) "puede" indica una posibilidad o una capacidad.

Es decir que si queremos organizar nuestro BCMS alineado con los aspectos "mandatorios" del estándar, debemos considerar TODOS los puntos en los que mencione "**shall**" y organizar nuestra estructura documental sobre la base de estos "shall".

No podemos en este libro, reproducir el detalle de los aspectos mandatorios que impone esta norma (no sería legal hacerlo pues, como todas las normas ISO, se tata de una norma de pago, con su respectivo copyright). A su vez concretamente en todos los puntos de la misma impone actividades y documentos a llevar a cabo, pero a los efectos que

tengáis alguna buena aproximación sobre la intención de la norma, a continuación presentamos un resumen de los aspectos mandatorios.

En la *sección 4* "Contexto de la Organización", se establecen varios puntos obligatorios en relación al establecimiento del BCMS, su organización y contexto, las partes interesadas, requisitos legales, los límites y aplicabilidad y su alcance.

Es decir, este primer documento mandatorio es la descripción detallada de la organización y lo que comprende este BCMS.

En la *sección 5* "Liderazgo" desarrolla los aspectos clave del compromiso y la política que debe seguir la alta dirección con el BCMS, los roles organizacionales, responsabilidades y de las autoridades.

En la *sección 6* "Planificación", nos presenta cómo lo desarrollado en 4 y 5 debe ser considerado para determinar los riesgos y oportunidades. Aquí ya entra de lleno en los temas concretos de la continuidad de negocio.

En la *sección 7* "Soporte" desarrolla como la organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del BCMS y las competencias de cada uno de ellos. Hace bastante hincapié en los temas de concienciación, cómo se deben realizar las comunicaciones internas, y por supuesto no puede faltar los detalles sobre la información documentada (que tal vez sea el punto clave de esta norma).

La *sección 8* "Operación". La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos, y para implementar las acciones determinadas, analizando el impacto empresarial y mantener una evaluación de riesgos actualizada que permita definir criterios de impacto y su medición. Al final del punto desarrolla las estrategias y soluciones de continuidad de negocio y las posibles respuestas. Este es otra sección que requiere alto grado de dedicación.

La *sección 9* "Evaluación de desempeño", desarrolla las medidas de monitoreo, medición, análisis y evaluación, los aspectos a considerar para la auditoría interna y finalmente cómo debe ser la revisión por la dirección.

La última *sección, la 10* "Mejora", se basa en la lógica de este ciclo PDCA y desarrolla justamente el punto "A" (Act), basado en las no conformidades y acciones correctivas que se vayan detectando y cómo establecer el ciclo de mejora continua sobre las mismas.

El detalle de este plan lo establece la norma **ISO 27031-2011** "**Gestión de la Tecnología de Información y Comunicación y obtención de Continuidad de Negocio**" (Guidelines for information and communication technology readiness for business continuity), esta norma es el reemplazo al **BS 25777**, y es como una herramienta técnica o, como su nombre lo indica, una guía de pasos, acciones y medidas a seguir para mantener el negocio "vivo". Reúne los dos conceptos de DRP y BCP. Desarrolla los temas fundamentales para las estrategias a seguir mediante la reducción del riesgo en la interrupción de las TICs. Como todas las normas ISO actuales se basa en el ciclo PDCA (ya desarrollado), por lo que si hemos estado siguiendo toda la propuesta de los capítulos de este libro, ya hemos avanzado gran parte de este camino. En este caso, como buena familia 27k, sigue adelante con la mejora continua de SGSI (Sistema de Gestión de la Seguridad de la Información).

La figura clásica que vemos en todas las presentaciones sobre esta norma es:

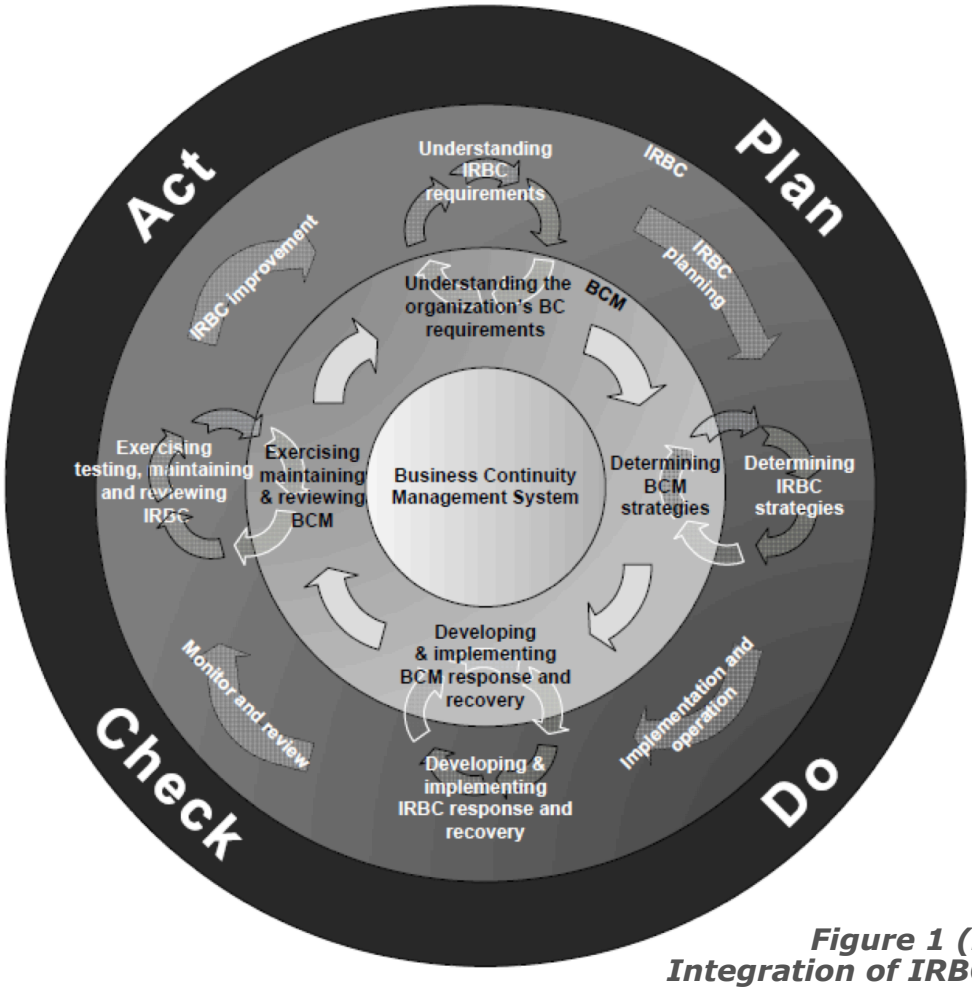


Figure 1 (ISO 27031)
Integration of IRBC and BCMS

En la figura anterior, se puede apreciar cada una de las actividades que propone esta norma.

Como novedad en esta inimaginable capacidad que tenemos para crear abreviaturas, ahora ISO nos ofrece una más... las viejas **TICs** de toda la vida, en estos nuevos estándares ha decidido llamarlas "**ICT**" (Information and Communication Technology) y como en esta norma ya confluyen el DRP y el PCN, ahora entonces veremos que se refiera a ellos como:

ICTDR (Disaster Recovery)

IRBC (I=ICT y RBC=Readiness for Business Continuity)

Los principios que propone esta norma son:

- Prevención de incidentes

- Detección de incidentes
- Respuesta
- Recuperación
- Mejora

Como parte de la familia 27K, esta norma amplía los puntos relacionados con BCP de la **ISO 27001-2017**, estos son desarrollados en el Anexo A (de la ISO 27001) y comprende los siguientes puntos:

A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio.

A.17.1 Continuidad de la seguridad de la información.

A.17.1.1 Planificación de la continuidad de la seguridad de la información

A..17.1.2 Implementar la continuidad de la seguridad de la información

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

A.17.2 Redundancias.

A.17.2.1 Disponibilidad de los recursos de tratamiento de la información

12.4. Gestión de la información (Clasificación y tratamiento).

Como mencionamos desde el principio del libro "la información es el bien más importante de la organización".

> **Recordad:** Lo crítico es la "Información"... no las Infraestructuras (*Capítulo 2*).

Si somos verdaderamente conscientes de estos párrafos, este es uno de los procedimientos sobre el que mayor esfuerzo deberíamos poner.

Hoy en día a la hora de implantar este procedimiento hay algunos aspectos que deberían ser la estructura raíz de este documento:

- Clasificación y tratamiento.
- Protección de la información almacenada y en tránsito.
- Información que contiene datos de carácter personal.
- Prevención de pérdidas de información.
- Propiedad intelectual y cumplimiento legal.

Desarrollemos cada uno de ellos:

12.4.1. Clasificación y tratamiento.

En mi opinión particular, creo que desde que somos niños vamos aprendiendo que hay información que puede compartirse con nuestra familia, otra con nuestros amigos, padres, profesores, parejas, hijos etc. Y otra que no debe mezclarse o salir de un determinado ámbito, pues puede costarnos muy caro. Este concepto tan absolutamente básico lo llevamos en nuestra sangre y, seguramente a todos nos ha sucedido, más de una vez…, que la misma trasciende, o se filtra de un entorno a otro, que no debía, y nos ha costado penitencias, peleas, suspensos, amonestaciones y en los peores casos hasta rupturas de por vida. Ni qué hablar de esos hackeas o intrusiones a nuestros ámbitos más privados donde guardamos agendas, diarios, fotos, etc.

Yendo a un ámbito profesional, se trata, ni mas ni menos, que volcar este infinita experiencia evolutiva a un ciclo PDCA (…*ya que estamos con ISO…*).

Concretamente debemos pensar o analizar sobre TODA la información que cuenta la organización, los siguientes conceptos:

- Qué: Grado de necesidad de acceso posee.
- A quién: Va dirigida o quién puede hacer uso de la misma.
- Cómo: Debe tratarse.
- Dónde: Debe ser empleada y almacenada.
- Cuándo: Está disponible.
- Atribuciones: Qué, quién y cómo puede o no puede tratarse la misma.

Desarrollemos con más detalle estos puntos.

- Qué: Grado de necesidad de acceso posee.

  La necesidad de acceso, en general suele establecerse en cuatro categorías:

  - Pública ***(PUB)***.
    Información disponible para todo tipo de público, interno o externo a la organización, conocido o anónimo.
  - Uso Interno (o privada) ***(PRIV)***.
    Información que está disponible para el personal de la organización, y no fuera de ella. Puede ser entregada a socios, partners, proveedores o clientes sobre los que se cuente con acuerdos de confidencialidad
  - Reservada (o restringida) ***(RES)***.
    Información que solo es necesaria para ciertas áreas o niveles de la organización, pero no a toda la empresa. En el caso de ser necesario compartirla en cualquier otra área de la establecida, necesita realizarse un flujo de aprobación, control y seguimiento de la misma.

- Secreta (o Confidencial) ***(SEC)***.

  Información de alta criticidad que debe ser sometida a la máxima protección. Su relevancia es tan alta que cualquier fallo en su seguridad ocasiona una alto impacto en la organización. Su acceso estará limitada a un número reducido de personas, las que llevarán el control de distribución y autorización para todo su tratamiento.

El aspecto más importante, y tal vez lo más difícil, en la clasificación de la información es no pecar por exceso, ni por defecto, pues una baja clasificación ocasionará fugas de la misma, pero también un exceso o sobre calificación tendrá como consecuencia excesivo freno, mala eficiencia, escaso rendimiento y, en el caso más frecuente, que paulatinamente se comience a no dar cumplimiento a los procedimientos.

En general se suele denominar como "Información Clasificada" a las dos últimas: Reservada (o restringida) y Confidencial (o secreta). Como cabe esperar esta información es la de mayor impacto en la organización y por ello requiere medidas de protección adicionales que deberán incluir al menos:

- Obligatoriedad de identificación y marcas.
- Restricciones de almacenamiento y transporte
- Directrices detalladas sobre permisos, roles, acceso, supervisión, etc.
- Autorizaciones para modificación, llevarla fuera de la organización, tiempos de empleo, proceder ante pérdida, destrucción de temporales y papeles de trabajo con la misma, envíos y recepción, marcas de agua, sellados de tiempo y criptografía, etc.
- Medidas adicionales de destrucción que impidan su recuperación.

Para el tratamiento de este información clasificada, el Centro Nacional de Inteligencia España (**CNI**) que ya hemos mencionado y de quien depende el **CCN**, también tiene otra dependencia llamada: Oficina Nacional de Seguridad (**ONS**) que

es responsable de velar por el cumplimiento de la Normativa relativa a la protección de la información clasificada, tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de tratados o acuerdos internacionales suscritos por España.

Un muy buen documento a tener en cuenta de esta entidad son las "**Normas de la Autoridad Nacional para la protección de la Información Clasificada**" que os recomendamos que leáis podéis descargar en el siguiente enlace:

https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf

- A quién: Va dirigida o quién puede hacer uso de la misma.

  La información por su contenido va dirigida a un público que en lo posible debe ser identificado y catalogado para poder, justamente, aplicarle las medidas de seguridad necesarias.

  Con independencia, y también en muchas veces en relación a su clasificación, una información puede ser dirigida en grandes líneas a diferentes grupos, dentro de los cuáles, se puede ser más específico aún. A continuación presentamos algunos ejemplos de agrupamientos:

  - Jerarquías: Directivos, gerentes, jefes, operarios, clientes, proveedores, etc.
  - Roles: Propietario, responsable, encargado, lectura, escritura/modificación, etc.
  - Grupos o perfiles: Técnicos, administradores, operadores, soporte, data entry, etc.
  - Áreas: Ingeniería, planificación, operación, financiera, marketing, ventas, compras, auditoría, etc.

  Sobre la base de la clasificación y los diferentes agrupamientos, ya es momento de plantearse las "**Restricciones de acceso**" que se deberán aplicar para cada uno de ellos pueda hacer uso adecuado de la

información que le corresponde y ninguna más, como tampoco ninguna menos.

- Cómo: Debe tratarse.

  Es natural volver a recordar conceptos de nuestra vida cotidiana. Hoy en día, todos somos conscientes (*o deberíamos serlo…*) de lo importante que es la información que nosotros gestionamos en WhatsApp, mails, SMSs, o en la nube. Seguramente hemos escuchado cómo se ha incrementado el nivel de confidencialidad de las conexiones al enviar estos datos o en el almacenamiento de los mismos. Por supuesto, en esta batalla de medidas y contramedidas, siempre hay brechas, fugas, intrusiones, etc. Pero creo que es claro para todos, que no es lo mismo la información cuando circula por las redes que cuando se almacena. Es decir, debo ser consciente o evaluar que cuando envío un correo electrónico, el mismo viaje por medio de conexiones seguras (https, túneles),

  El cómo nos presenta dos grandes posibilidades:

  - Almacenada o en tránsito.
  - Información en papel o en formato electrónico.

  Tanto para la información en papel, como para la electrónica debe haber una clara definición de su etiquetado y nomenclatura para poder identificar de forma eficiente, rápida y segura de qué se trata cada una de ellas.

  Otro aspecto a tratar en este cómo, es el ciclo final de una información, es decir su "**Destrucción**". Más peligroso que la pérdida de información, es no saber qué ha sido de ella, por lo que toda información crítica de la organización debe respetar a rajatabla una serie de pasos que identifiquen claramente cuando la misma finalizó con su ciclo de vida y es destruida, para que quede debidamente registrado este paso. Toda información destruida deberá quedar registrado un detallado histórico de su ciclo de vida completo, si la información es reservada o confidencial este último párrafo cobra especial interés.

Existe una norma **BS** (British Standard) **EN 15713** "Secure Destruction of Confidential Materials", que desde febrero de 2010 tiene su versión española: **UNE-EN 15713:2010** "Destrucción segura del material confidencial. Código de buenas prácticas", que proporciona recomendaciones para gestión y control de la destrucción de material de carácter confidencial de forma segura y sin peligro. Esta norma establece: clases y niveles sobre los que establece las diferentes acciones y medidas a tener en cuenta a la hora de la destrucción con altísimo grado de detalle, llegando a estipular hasta el ancho en milímetros que debe ser triturada en los casos de información en papel, o cortado en el caso de soportes físicos de información electrónica, o el tipo de acreditación que debe requerirse a una empresa externa si se contrata este tipo de servicios. Si el negocio de vuestra organización depende en alto grado de este tipo de información este documento es un muy buen referente.

Un último tema que no puede ser dejado de lado ene este procedimiento es cómo se trata y/o entrega información en los casos que lo requiera alguna autoridad gubernamental, policial o judicial. Las bases y regulaciones legales de cada país son diferentes al respecto, por lo que se deberá analizar la misma y dejar estos pasos perfectamente documentados. Todo empleado de la organización deberá conocer al detalle este aspecto.

- Dónde: Debe ser empleada y almacenada.

  Sobre este punto siempre prefiero tomar como punto de partida las normas **ISO** que permanentemente hacen referencia a un sistema de gestión documental. Este tipo de plataformas, permiten organizar desde la jerarquía de la misma, hasta el control de accesos, cambios, alta, baja y modificaciones, versionado, copias de respaldo y restauración. En la experiencia de trabajo, si bien en general no me gusta hacer publicidad a productos

comerciales, debo reconocer que como muy buen ejemplo está **SharePoint** de Microsoft, que se trata de un producto muy bien diseñado para este fin, también debo mencionar que en la mayoría de los casos he podido apreciar que no se suele aprovechar al máximo sus prestaciones. Otro producto open source que es también recomendable es **Alfresco**.

- Cuándo: Está disponible.

  Como hemos mencionado, el ciclo de vida de la información debe ser uno de los factores clave de este procedimiento. En seguridad informática, este aspecto guarda directamente relación con una de las cinco palabras cláveme de la regla mnemotécnica **ACIDA** (autenticación, Confidencialidad, Integridad, Disponibilidad, Accounting (o trazabilidad)). En este caso, la información debe estar disponible: cuándo y a quién la necesite. De nada sirve un procedimiento, directiva, manual o guía, si cuando hay falta no se lo puede encontrar, o quien lo necesita tiene el acceso restringido. Por otro lado, también es nefasto que tenga acceso aquel que no deba, y pueda verlo o descargarlo.

  A partir que un documento es aprobado por su responsable y entra en vigor, comienza el instante cero de esa información. En ese preciso instante ya debe tener clasificado y catalogado quién puede, o no, acceder a la misma. A su vez en ese sistema de gestión documental, debe estar definido y claramente difundido cuál será su ubicación y permisos.

  El ciclo de vida de la información debe contemplar al menos las siguientes fases:

  - Creación
  - Clasificación y etiquetado
  - Aprobación
  - Almacenamiento

- Compartición
- Ubicación o localización
- Actualización
- Control de cambios
- Destrucción y archivo histórico

- Atribuciones: Qué, quién y cómo puede o no puede tratarse la misma.

  Los diferentes roles y permisos que se han mencionado en los párrafos anteriores deberán tener claramente especificadas sus atribuciones para que el ciclo de vida de la información pueda mantenerse de acuerdo a sus fines. Es decir, debe quedar perfectamente establecido, quien la genera, participa y aprueba, y luego quien puede emplearla (leer), modificar y derogar.

12.4.2. Protección de la información almacenada y en tránsito.

Debe quedar establecida la metodología a seguir para cada tipo de información en papel/electrónico y almacenada/tránsito. En este punto, se deberá desarrollar con toda claridad, y de acuerdo con su clasificación, cómo debe tratarse cada una de ellas. Desde los aspectos de cifrado hasta los métodos de transporte físico que se permitirán o no, embalajes, sobres, cajas fuertes, túneles, protocolos, etc.

12.4.3. Información que contiene datos de carácter personal.

Tomando como punto de partida la regulación Española que ha sido muy robusta con los datos personales, en sus inicios se basó en la Ley Orgánica de Protección de Datos (**LOPD**) y actualmente por la GDPR (Regulación Europea de Protección de datos Personales).

A partir del año 2018, esta última establece todas las medidas a adoptar para cualquier información que puede contener un dato personal, estableciendo claramente las distinciones entre la persona física y los datos que se corresponden a empresas o comercios.

Estas regulaciones, tienen por finalidad proteger la información privada de las personas y evitar que desde cualquier ámbito se pueda tratar con la misma, u obtener beneficios de cualquier tipo. Considero que la GDPR es una de las regulaciones mas maduras sobre este tema, no podemos en este libro tratarla con el detalle que merece, pero es de dominio público y explicada en muchos foros y páginas de Internet. La única intención de hacer mención del tema en estas páginas, es despertar consciencia sobre la importancia que debe tener, si en nuestra organización nos encontramos con información de este tipo. Esta información es prioritaria y debe ser considerada con especial interés, pues independientemente de las multas y sanciones que pueden caernos, se trata justamente de un tipo de datos especialmente relevantes y por supuesto, mucho más aún, si se guardan relación con información de salud, política, religiosa o sexo.

Nuestra recomendación es que dediquéis un buen tiempo a analizar estas regulaciones y luego, apliquéis los conceptos de las mismas en vuestra organización con la mayor meticulosidad posible, estéis o no en la Unión Europea, y por supuesto la sincronicéis con las regulaciones del país en que se encuentre vuestra empresa.

12.4.4. Prevención de pérdidas de información.

Este punto es muy conocido por sus siglas en inglés **DLP** (Data Loss Prevention).

Nuevamente como se comprenderá esta actividad debe centrarse principalmente en la información clasificada, pues es ella la que genera alto impacto si pierde su carácter de Confidencialidad, e inclusive ante fallos de acceso, pues a partir de un acceso indebido ya se tiene el riesgo de una potencial ruptura de su Confidencialidad también.

Las fuentes más conocidas de fuga de información son:

- Impresoras y FAX.
- Correo electrónico.
- Mensajería.
- Páginas y navegación Web.
- Dispositivos extraibles.

- Bases de datos y servidores de archivos.
- Servidores de backups.
- Copias de seguridad.
- Teletrabajo.

Hoy en día, las empresas que deciden poner interés en estas medidas cuentan con una buena cantidad de software para la prevención y detección de fugas. Este tipo de herramientas, monitorizan nuestras redes y sistemas de TI buscando brechas o potenciales fugas y tienen la posibilidad de hasta bloquear lo que consideran peligroso.

Dejando de lado las medidas estándares como firewalls, control de acceso, autenticación, etc. Existen también una serie de medidas específicas para prevención de fugas de información, que son justamente las que emplean estas herramientas. Estas medidas, se basan en algoritmos y escuchas de tráfico que permiten ir ajustando la conducta "normal" de nuestros flujos de información y detectar, alertar, o bloquear cuando algo de ello parece ser anómalo.

Al solo efecto de poder evaluar alguna soluciones, se presentan a continuación algunas opciones de software y herramientas.

CheckPoint comenzó con un producto llamado "DLP Software Blade" y ahora lo presenta como algo integrado en la "familia Infinity" con varias opciones y cada día mejora sus prestaciones. https://www.checkpoint.com/products/data-loss-prevention/

Digital Guardian, es un empresa con más de diez años de experiencia en el tema y ofrece una amplia gama de soluciones.

https://digitalguardian.com/es

End Point Protector, es otra empresa que ofrece diferentes opciones.

https://www.endpointprotector.es

Si tienes deseos de investigar y ser partícipe en el tema, te invitamos a que veas el proyecto **OpenLDP** que puede resultarte provechoso e interesante como todos los desafíos Open Source.

https://code.google.com/archive/p/opendlp/

12.4.5. Propiedad intelectual y cumplimiento legal.

Dentro de la clasificación de la información hay un concepto que debe ser considerado especialmente, se trata de la propiedad intelectual de la misma.

Sobre este aspecto hay dos variantes a considerar. La primera de ellas es sobre toda información generada por personal de la organización, la misma si está relacionada con el trabajo que este desarrolla, debe quedar siempre claramente establecido en los contratos que es propiedad intelectual de la organización. Este tema ha sido foco de conflictos en reiteradas oportunidades, en particular sobre desarrollos de software que han sido excesivamente novedosos y lucrativos. Si este tipo de cláusulas no son identificadas desde el principio, existe un alto riesgo. En algunas ocasiones, se produce el hecho del crecimiento sobre algún desarrollo basado en propiedad intelectual de personas o grupos, que se toman como punto de partida, o al revés que luego se derivan de una base de software. En estos casos, también debe quedar claro contractualmente los porcentajes de participación y distribución de la propiedad intelectual de los mismos. En cualquier caso, la clasificación de toda la información generada establecerá la propiedad intelectual de la misma.

La segunda variante a considerar sobre propiedad intelectual, es que el personal de la organización debe ser consciente y conocer al detalle la propiedad intelectual del material que emplea, tanto en el uso legal de software, como en que sus propios desarrollos y trabajo cotidiano no afecten la propiedad intelectual de otras empresas u organizaciones. Aquí es donde entran en juego particularmente las regulaciones legales de cada país e institución, las cuales, de más está decir, deben cumplirse rigurosamente.

En resumen, la propiedad intelectual, es un aspecto que debe ser considerado en toda información de la organización, tanto en la propia como en la externa, con los productos y servicios que formen parte de nuestra actividad actividad

Como ya hemos puesto de manifiesto las guías del **ENS**, en esta caso merece la pena dedicarle un buen tiempo al "**PROCEDIMIENTO DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA - PR20**", que se puede descargar en:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/539-ccn-stic-822-procedimientos-de-seguridad-anexo-ii/file.html

12.5. Gestión de copias de respaldo y recuperación.

Los aspectos básicos de este proceso lo hemos desarrollado ya en el libro "**Ciberseguridad, una Estrategia Informático/Militar**" y puede verse en detalle en el punto: 6.2.5. Gestión de Backup, en esa sección ya hacemos mención al mensaje más importante de este proceso:

> *"Dado que el backup es el último recurso en caso de producirse una situación de pérdida de datos, es muy importante definir un procedimiento de backup que sea común a todas las unidades de la empresa".*

También hemos desarrollado en este libro dos ideas fundamentales sobre este proceso: **RPO** y **RTO**, cuando desarrollamos en el capítulo **8. Matriz de Resiliencia**, el Grupo 2: "Ciclo de vida".

Jamás dejemos de lado que el pilar más robusto que tiene la "Ciber resiliencia" son las copias de respaldo.

Como vinimos desarrollando a lo largo del libro, no todas la información tiene el mismo valor, por esa razón presentamos al principio el "Análisis de riesgo", luego la "Matriz de Resiliencia", con estos pasos, fuimos identificando la criticidad de nuestros activos, siempre sobre el concepto que dijimos al principio: "Lo crítico es la Información, no las infraestructuras".

Una buena estrategia de gestión de copias de respaldo y recuperación, es aquella que prioriza lo crítico, y luego sigue avanzando sobre el resto siempre sobre la base de su nivel de riesgo e impacto. No es una buena práctica implementar backups de toda la organización, tratando todo por igual, esto es un gasto innecesario que genera desgaste y pérdida del norte.

Sobre este proceso, si la organización es grande y posee diferentes tipos de sistemas, redes, plataformas e infraestructuras, es una muy buena medida, generar un procedimiento global para toda la organización que defina e imponga las normas y pasos fundamentales de obligado cumplimiento y luego desarrollar guías o manuales más técnicos que sobre la base del anterior, especifiquen las medidas concretas para cada área o infraestructura. Con este desglose de documentación, se logra que toda la empresa siga una metodología común que de cumplimiento a lo que imponga la dirección, y luego sea posible aplicar esas líneas mandatorias de

forma concreta y con mayor grado de detalle a cada infraestructura específica.

***MENSAJE ESPECIAL**: Si la información es CRÍTICA, una muy buen idea es mantener siempre alguna copia reciente "Off line" (fuera de línea).*

(Un ¿buen? intruso, o atacante, pondrá un gran esfuerzo en localizar nuestros backups, y cuando quiera hacer daño intentará destruir todos los que encuentre).

Sobre la información clasificada, se deben al menos considerar los siguientes conceptos:

- Detalle de la información que se respalda
- Medidas especiales sobre respaldo de información personal
- Sistemas origen que se respaldan
- Sistemas y servidores que almacenan las copas de respaldo
- Ubicaciones físicas
- Personal responsable de cada acción
- Permisos de acceso a copias de respaldo
- Metodologías de solicitud de recuperación
- Frecuencia mínima de los respaldos
- Metodología de los respaldos
- Metodología de verificación, monitorización y restauración
- Pruebas y test de recuperación periódicos
- Registros y reportes
- Períodos de retención
- Metodología de rotación de copias
- Información almacenada fuera de línea
- Metodología de destrucción de respaldos
- Medidas de confidencialidad (criptografía) a aplicar
- Metodología de custodia de claves
- Almacenamientos recurrentes
- Revisión y actualización de metodologías de respaldo y recuperación

La norma **ISO/UNE-27001-2017**, establece en sus objetivos de control en el Anexo A, el punto A.12.3 "Copias de Respaldo", en el mismo establece de forma mandatoria este control: "*Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada*".

Volviendo al **ENS**; la guía **CCN-STIC-822**. "Procedimientos de Seguridad en el ENS", en su Anexo III presenta el "**Procedimiento de generación de copias de respaldo y recuperación de la Información - PR30**", que puede descargarse en:

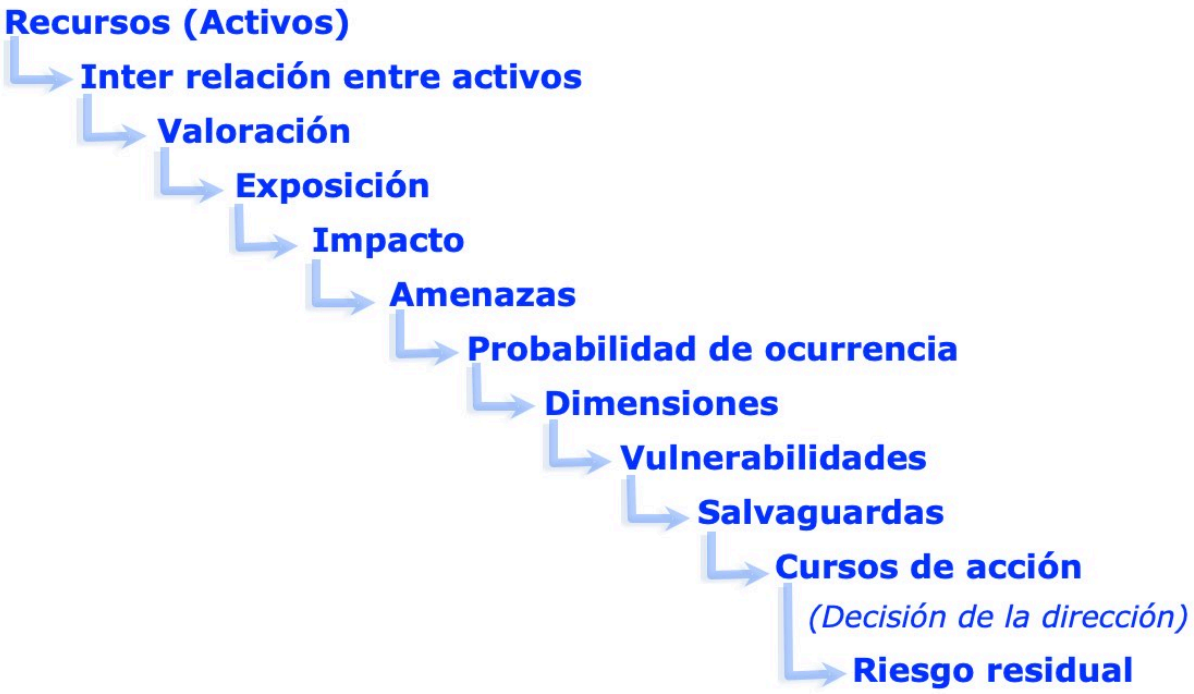
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/540-ccn-stic-822-procedimientos-de-seguridad-anexo-iii/file.html

12.6. Gestión de riesgos.

En el Capítulo **6. Análisis de Riesgo de Resiliencia**, ya comenzamos a desarrollar este tema, como este libro se refiere a resiliencia, recordemos las "**4R**" (*robustness, redundancy, resourcefulness, and rapidity*) que mencionamos en ese capítulo. Nuestro proceso de análisis de riesgo, si queremos tener una infraestructura "Ciber resiliente", debe estar basado en estas "4R".

De las metodologías presentadas en el capítulo 6, en el libro desarrollamos con mayor grado de detalle "**MAGERIT**", pero por supuesto que el lector puede aplicar la que desee. En nuestro caso, para mantener la línea de este libro, presentaremos la lógica de este proceso basada en esta metodología.

Recordemos que en grandes líneas la secuencia básica de pasos es:



Por lo tanto, sin lugar a dudas, este proceso debe describir detalladamente cómo se realizan estas acciones en la organización, tema que está bastante desarrollado en el capítulo 6.

Como detalle específico de una análisis de riesgo resiliente, en el capítulo **7. Análisis de Resiliencia en Redes y Sistemas**, hicimos bastante hincapié en cómo llevar a cabo este "ciclo de vida". Tal cual dice MAGERIT dar respuesta a "*lo que se denomina "Proceso de Gestión de Riesgos", aconsejando que suele ser prudente una aproximación iterativa*". Es decir, estamos hablando que esta gestión de riesgos es una actividad "viva" y permanente.

En el capítulo **8. Matriz de Resiliencia**, ya concretamos la parte final del análisis de riesgo en tres grupos:

- Objetivos y gestión
- Ciclo de vida
- Arquitectura de ciberdefensa

Sobre estos tres grupos, cuantificamos nuestros activos críticos, identificando de forma concreta nuestros principales riesgos, para poder dar paso el capítulo **9. Estrategias Resilientes en Redes y Sistemas**, donde la alta dirección podrá adoptar la decisión que crea conveniente sobre indicadores claros, concretos y calculados con una metodología robusta y comprensible.

Como no podía faltar, en el capítulo **10. Ciclo de vida**, se desarrolla este aspecto fundamental de un sistema resiliente, y se exponen las métricas y metodologías necesarias para poder evaluar con la periodicidad que se considere oportuna, cualquier tipo de desvío, y aplicar las medidas o correcciones pertinentes.

Toda esta introducción, tiene la intención de invitaros a que reflexionéis sobre lo que hemos ido desarrollando y toméis estos conceptos como base de la documentación de este proceso de "gestión de riesgos", pues aquí tenéis desarrollado el cuerpo de este documento, por supuesto ajustándolo a vuestras organizaciones.

¿Qué otros aspectos debe contemplar este documento?

a. Roles y responsabilidades.

Lo primero que se debe tener en cuenta es que todas las personas dentro de la organización tienen la responsabilidad de contribuir a la gestión de riesgos, pero por supuesto hay que especificar con mayor detalle:

- Propietario de los activos.
- Analistas y responsables de la gestión del riesgo.
- Especialistas técnicos.
- Encargados de tratamiento (de riesgos, de datos, de datos personales, etc.).

b. Periodicidad.

Según las necesidades de la organización y teniendo como principal referente a la legislación local, cada área de la organización deberá definir un plazo máximo para las realizaciones, revisiones y evaluaciones del riesgo de su área.

c. Plan de tratamiento del riesgo.

Se debe exponer aquí cómo y dónde se registrarán los detalles sobre las acciones de tratamiento del riesgo.

d. Difusión.

El análisis de riesgo es un conjunto de medidas y acciones que contienen mucha información clasificada, justamente estamos exponiendo los activos, responsables, sus criticidades, focos de inversión y esfuerzos principales y cuáles son los impactos mas graves que podemos sufrir. No es necesario que toda esta información esté disponible abiertamente, sino que se deberá evaluar con mucha rigurosidad qué es lo necesario a difundir y que no, y, cada parte de ello considerando quién debe tener acceso.

e. Resultados.

- A quién se reportan los pasos, medidas y acciones derivadas del análisis de riesgo.
- Qué tipo de evidencias son necesarias.
- Qué tipo de tratamiento se realizará con las métricas y KPIs definidos.
- Tiempos y medidas de mitigación, incluyendo los responsables de esto.

Como documentos de referencia para la redacción de este procedimiento podemos citar los siguientes:

- norma **UNE-EN 31010:2011** Gestión del riesgo - Técnicas de apreciación del riesgo.
- norma **UNE-ISO 31000:2018** Gestión del riesgo - Directrices

12.7. Gestión de incidentes.

Este tema también ha sido desarrollado en el libro "**Ciberseguridad, una Estrategia Informático/Militar**" en el punto 6.2.6. Gestión de Incidencias. En esta anterior publicación hacíamos hincapié en dos conceptos originados en la **RFC-1244** que hoy queremos volver a rescatar:

- Protect and Proceed (Proteger y proceder)
- Pursue and Prosecute (Seguir y perseguir)

Si estamos desarrollando conceptos resilientes, no podemos ahora considerar la primer estrategia, pues tal cual expresamos en su momento, proteger y proceder, se basa en una reacción inmediata y poco madura en la que apagamos, desconectamos, logrando con ello detener el problema, pero por supuesto, cuando volvamos a activar todo el problema seguirá latente allí. La capacidad de resiliencia, tal cual fuimos abordando en nuestras diez reflexiones desde el inicio de este libro, se basa en poder recuperar de forma elástica y confiable nuestras redes y sistemas de TI, esto solo se logrará pudiendo detectar temprano, analizar el hecho en detalle, recuperarse y erradicar el problema. Evidentemente lo que debemos desarrollar es la estrategia de "seguir y perseguir".

Permitidme ahondar un poco más en los conceptos de esta vieja RFC-1244 sobre seguir y perseguir. En el punto el 2.5. de la misma establece que (SIC):

> *1. If assets and systems are well protected.*
>
> *2. If good backups are available.*
>
> *3. If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.*
>
> *4. If this is a concentrated attack occurring with great frequency and intensity.*
>
> *5. If the site has a natural attraction to intruders, and consequently regularly attracts intruders.*
>
> *6. If the site is willing to incur the financial (or other) risk to assets by allowing the penetrator continue.*
>
> *7. If intruder access can be controlled.*

8. *If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.*
9. *If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.*
10. *If there is willingness on the part of management to prosecute."*
11. *If the system adminitrators know in general what kind of evidence would lead to prosecution.*
12. *If there is established contact with knowledgeable law enforcement.*
13. *If there is a site representative versed in the relevant legal issues.*
14. *If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit."*

Quedémonos con los puntos clave de estos conceptos:

1. *Si los activos y sistemas están bien protegidos.*
2. *Si hay buenas copias de seguridad disponibles.*
3. *Si el riesgo para los activos (o recursos) se ve compensado por la disrupción causada por las penetraciones presentes y posiblemente futuras.*
7. *Si el acceso de intrusos puede ser controlado.*
8. *Si las herramientas de monitorización (o supervisión) están suficientemente desarrolladas para que el seguimiento valga la pena.*
9. *Si el personal de soporte es lo suficientemente capaz y tiene el conocimiento del sistema operativo, las utilidades (o aplicaciones) relacionadas y los sistemas para que el seguimiento valga la pena.*
10. *Si hay voluntad por parte de la dirección de perseguir.*

11. Si los administradores de sistemas saben, en general, qué tipo de evidencia son clave para la persecución.

12. Si existe contacto con las autoridades competentes.

13. Si en nuestra organización hay un representante con conocimiento en aspectos legales.

14. Si el sitio (plataforma/host/infraestructura) está preparado para una posible acción legal de sus propios usuarios, si sus datos o sistemas se ven comprometidos durante la búsqueda o seguimiento.

El mensaje que nos transmite esta RFC podríamos resumirlo en:

- Nivel de bastionado de nuestras redes y sistemas de TI.
- Copias de respaldo y recuperación.
- Nivel de mitigación de riesgos que hemos asumido.
- Medidas o herramientas de seguridad.
- Grado de involucramiento de la dirección en temas de seguridad.
- Know how de nuestro personal, y generación y resguardo de evidencias.
- Soporte legal.

Estos aspectos son el punto de partida para una estrategia resiliente que nos permite "seguir y perseguir" un incidente de seguridad.

Una infraestructura resiliente debe contar con un implantado y robusto procedimiento de gestión de incidentes, pues ya lo hemos puesto de manifiesto:

Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas"

John Chambers (CEO de

Un incidente de seguridad con toda certeza ya nos ha sucedido y si no lo vemos así es solamente porque no nos hemos enterado. La gestión de los mismos hoy en día debe estar ajustada al detalle, caso contrario nuestra organización no será ciber resiliente.

Como ya hemos desarrollado en detalle el tema de riesgos, estamos en situación de entender que tipo de ciberamenazas son las de mayor impacto en nuestra organización. Una de las primeras actividades es poder desarrollar una metodología de análisis, entendimiento e inteligencias sobre estas amenazas, con el objetivo de poder anticiparse todo lo posible a las mismas. Esto comprende todas las medidas preventivas, proactivas y el desarrollo de acciones previstas y de ser posible ensayadas o practicadas, en caso de concretarse cualquiera de ellas.

Cuando la organización tiene la capacidad suficiente, la implementación de un **CIRT** (Computer Incident Response Team) es una de las primeras medidas a adoptar. Si se puede poner en marcha, este centro será el responsable de la respuesta y gestión de cualquier tipo de incidentes, dedicando gran parte de su tiempo normal de actividad a la ciberinteligencia y a la preparación ante incidentes.

Este procedimiento debe describir en detalle cómo se aborda (paso a paso) la gestión de cualquier tipo de incidentes de seguridad, desde la formación necesaria a todo el personal de la empresa, la alarma primera, la clasificación, el tratamiento, hasta el cierre del mismo. Estos pasos, deben contemplar al menos:

- Clara definición de "incidente" para toda la organización.
- Alerta y contacto.
- Observación del mismo.
- Metodología de escalado y cadena de llamadas.
- Recopilación, proceso y distribución de información.
- Metodología de seguimiento de incidente (seguir y perseguir)
- Evaluación de la situación, incluyendo el pronóstico.
- Planificación de acciones.
- Toma de decisiones y comunicación de las decisiones tomadas.
- Implantación de las decisiones.

- Recogida de información sobre resultados y medidas de control.
- Tareas post incidente.
- Proactividad e investigaciones forenses.
- Gestión de medios de comunicación y prensa.
- Gestión de información ante autoridades.

Como siempre analicemos las normas internacionales sobre este tema. El principal referente que pertenece a la familia ISO 27000, es **ISO/IEC 27035:2016** "Information technology — Security techniques — Information security incident management" (gestión de incidentes de seguridad de la información).

En realidad esta norma consta de dos partes:

ISO/IEC 27035-1:2016 Gestión de incidentes de seguridad de la información - Parte 1: Principios de gestión de incidentes

Esta primera parte describe los conceptos y principios que sustentan la gestión de incidentes de seguridad.

Presenta cinco fases:

1. Planificar y preparar: establecer una política de gestión de incidentes de seguridad de la información, formar un equipo de respuesta a incidentes (CIRT).
2. Detección e informes: metodología para la detección y para informar "eventos" que pueden ser o convertirse en incidentes.
3. Evaluación y decisión: metodología para evaluar la situación y determinar si de hecho se trata de un incidente o no.
4. Respuestas: contener, erradicar, recuperarse y realizar el análisis forense del incidente.
5. Lecciones aprendidas: realizar un ciclo de vida en la gestión de los riesgos, como consecuencia del incidente experimentado.

ISO/IEC 27035-2:2016 Gestión de incidentes de seguridad de la información - Parte 2: Directrices para la planificación y preparación para la respuesta ante incidentes.

Esta parte tiene como objetivo que la organización esté lista para responder adecuadamente a los incidentes de seguridad que puedan ocurrir. Después de las secciones introductorias siguen 8 cláusulas:

4. Establecimiento de una política de gestión de incidentes de seguridad.
5. Actualización de las políticas de seguridad de la información y gestión de riesgos.
6. Creación de un plan de gestión de incidentes de seguridad.
7. Establecimiento de un equipo de respuesta a incidentes.
8. Definiciones técnicas y otro tipo de soporte.
9. Crear conciencia y formación sobre incidentes de seguridad.
10. Poner a prueba o realizar ejercicios sobre el plan de gestión de incidentes de seguridad.
11. Experiencias o lecciones aprendidas.

Otra norma que debemos citar también es **ISO/UNE 27002**, en su punto: **A.13** "Administración de los incidentes de seguridad" propone cinco controles que agrupa, y subdivide en:

Reportes de eventos de seguridad de la información y debilidades.

Como su nombre lo indica, este apartado define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas. Estas metodologías deben ser ágiles, por lo tanto se presupone el empleo de herramientas automatizadas que lo hagan. En estos momentos se poseen muchas de ellas.

En concreto para que estos controles puedan funcionar de manera eficiente, lo mejor es implantar herramientas de detección de vulnerabilidades, ajustarlas a la organización, para saber con total certeza dónde se es débil y donde no, y a través de estas desarrollar un mecanismo simple de difusión de las mismas a los responsables de su administración y solución, los cuales deberán solucionarlas o justificar las causas para no hacerlo, ante lo cual, esta debilidad pasará a ser tratada por el segundo grupo de este control, es decir una metodología de detección de intrusiones, que será la responsable de generar la alerta temprana, cuando una de esas debilidades sea explotada por personal no autorizado. Estas alertas necesitan también un muy buen mecanismo de gestión, para provocar la respuesta inmediata.

Administración de incidentes de seguridad de la información y mejoras.

Si se poseen los dos mecanismos mencionados en el punto anterior, la siguiente tarea es disponer de una metodología de administración de incidentes, lo cual no es nada más que un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas. Todo esto no es eficaz si no se realiza la preparación adecuada, por lo tanto es necesario difundirlo, practicarlo y SIMULARLO, es decir generar incidentes que no hagan peligrar los elementos en producción, tanto sobre maquetas como en planta y poner a prueba todos los eslabones de la metodología. Seguramente aparecerán fallos, zonas grises o brechas de seguridad metodológicas, las cuales la mejor manera de solucionarlas es en "situaciones de paz" y no durante un conflicto real… como se puede apreciar he escrito en terminología muy militar, pues esto no es ni más ni menos que lo que hacen (o deberían hacer….) durante todo el tiempo de paz las fuerzas armadas, "prepararse para incidencias", esta actividad no puede ser improvisada cuando llega la misma sino, no hace falta ser militar para deducir que será catastrófico. La preparación militar, en los casos defensivos hace principalmente esto, es decir analizar las posibles

metodologías que puede aplicar un enemigo y practicar su contramedida, esto es el entrenamiento militar y a su vez son los denominados "ejercicios militares" en el terreno o en mesas de arena (Léase planta y/o maqueta), que no son otra cosa que simulaciones sobre qué sucedería si reacciono des esta forma u otra. La doctrina militar es milenaria, tiene millones de situaciones vividas, practicadas y estandarizadas, por así llamarlas, por los tantos en los casos en que su analogía con la informática es evidente, no se debe re inventar la rueda, sino aprovechar lo que ya existe, y la preparación ante incidencias es uno de los casos más evidentes de esto. Existe un muy antiguo refrán que dice "*Si quieres vivir en paz, prepárate para la guerra*". Es decir, si quieres evitar problemas de seguridad, prepárate para ellos.

Como es lógico, lo ideal es la gestión óptima del incidente, habiendo podido prevenirlo, o al menos haber minimizado su impacto. Esto, en la realidad no siempre es posible y sabemos perfectamente que las condiciones tecnológicas cambian minuto a minuto, abriendo permanentemente nuevas posibilidades para bien y/o para mal de nuestra infraestructura de seguridad. Por cualquier razón, e inclusive en el mejor de los casos, una de las actividades más importantes desde el punto de vista de la ciberresiliencia será tener en cuenta un punto que acabamos de mencionar en el capítulo "**Proactividad e investigaciones forenses**".

12.8. Gestión de cambios y actualizaciones.

El proceso de gestión de cambios es el que garantiza la estabilidad de nuestra infraestructura a medida que evoluciona o se actualiza. Una mala implementación, o la inexistencia del mismo, es uno de los mayores errores en una infraestructura de redes y sistemas de TI. En nuestra experiencia hemos visto un sinnúmero de incidentes de alto impacto generados por cambios realizados fuera de ventana, sin los permisos necesarios, sin alertar al NOC o SOC, sin la realización correcta de preparación para un rollback, sin haber realizado pruebas en maqueta, sin la monitorización pertinente, etc. Este tipo de procederes pone en peligro toda la organización y a su vez en muchas oportunidades quedan en funcionamiento plataformas o dispositivos, sobre los cuáles aún no se poseen las medidas de seguridad actualizadas dejando brechas en los mismos que pueden impactar en cualquier otro ámbito si no se ha seguido un procedimiento estricto y en particular cuando los cambios son relevantes o críticos.

El proceso de gestión de cambios debe asegurar que los mismos estén justificados, no debiliten el nivel de seguridad, la calidad alcanzada, ni la disponibilidad de las redes e infraestructuras de TI.

Una secuencia natural para este procedimiento es la siguiente:

- Conformación de un comité de cambios.
- Solicitud de cambios.
- Responsables.
- Definición del flujo.
- Definición de los requisitos de seguridad de cambios.
- Identificación del cambio.
- Actuaciones ante cambios de emergencia.
- Clasificación.
- Estado del cambio.
- Registro.
- Evaluación de impactos potenciales.
- Definición de responsables.
- Planificación del cambio.
- Procedimiento de marcha atrás (rollback).
- Plan de pruebas.

- Empleo de maquetas y pre-producción.
- Ejecución del cambio.
- Evaluaciones del cambio.
- Paso a producción del cambio.
- Bitácoras de cambios.
- Actualización de documentación posterior al cambio.
- Mantenimiento del control de versiones.

Expliquemos con un poco más de detalle cada uno de ellos.

- Conformación de un comité de cambios.
  El comité de cambios será el órgano que autorizará o no cada cambio a realizar.
  Cuando la organización es grande, este comité es imprescindible y en particular cuando el proceso se encuentra debidamente implementado y se tiene experiencia sobre la criticidad de los mismos, el trabajo del Comité es fundamental.
  Como se verá más adelante, no es necesario que el mismo deba participar de todos los cambios, solamente de aquellos que potencialmente son evaluados con un riesgo o impacto alto para la empresa, el resto de los cambios puede llevarse a cabo sin su intervención, por supuesto cuando se tiene la garantía de su baja criticidad.
  El Comité de cambios en empresas grandes y de alto dinamismo, puede reunirse semanalmente en un horario preestablecido, y es en esa oportunidad donde se tratan y aprueban o no la cola de cambios semanal. Una vez aprobados en esa fecha hora, los gestores de cambio continúan con la operativa de los mismos.
  El modelo a seguir para la conformación de un comité de cambios es que esté constituido por:
  - Alto responsable de red.
  - Alto responsable de Sistemas de TI.
  - Alto responsable del área de seguridad.
  - Responsable legal.
  - Responsable de protección de datos personales.

- Solicitud de cambios.

Cualquier área de la organización podrá solicitar un cambio, siguiendo el flujo que deberá ser definido con máximo detalle. Este será el punto de partida normal de los mismos.
Cualquier otro cambio puede iniciarse también por razones de control de obsolescencia o parcheado, como así también por incidentes o razones de emergencia.
Todas estas situaciones cuanta mayor previsión y definición posean en el flujo, más robusto hará el procedimiento.

- Responsables.
  a. Solicitante: Cualquier área de la organización.
  b. Propietario: Responsable de la infraestructura sobre la que se realizará el cambio. Puede ser uno o varios.
  c. Gestor del cambio: Persona responsable de la gestión de ese cambio.
  d. Comité de cambios: Órgano responsable de velar por el cumplimiento del procedimiento, en particular para cambios de criticidad alta y crítica.
  e. Terceros: Este actor cobra especial interés cuando forma parte del flujo de cambio y/o es responsable de alguna de sus fases. Si es este el caso, debe ser considerado con mucha atención los acuerdos de nivel de servicio (SLA) que se tiene contratado con los mismos.

- Definición del flujo.
  Este paso es fundamental a la hora de poder diferenciar con máxima claridad los pasos a seguir. Sobre la base de la criticidad y prioridad que tenga un cambio, deberá seguir un camino u otro. No tiene sentido que para cambios de baja criticidad se deba convocar el comité de cambios, ni tampoco en general para los de emergencia (con excepción de los críticos, donde podrá participar y convocarse de forma urgente).
  Este flujo suele costar bastante tiempo en "ajustarse" debidamente en cualquier organización, pero debe hacerse y mejorarse hasta que funcione a la perfección, pues cuanto más "mandatorio" sea el mismo, y sin dejar opciones alternativas, ni caminos secundarios, más seguros serán los cambios dentro de la organización.

El proceso de aprobación de cambios deberá detallarse en este punto, siendo necesario y mandatorio para todo cambio que se considere de nivel alto o crítico.

- Definición de los requisitos de seguridad de cambios.
  El área de seguridad debe poseer potestad bloquean de cambios siempre. Es decir, en el flujo de todo cambio deberá participar "sí o sí" el área de seguridad, dando su aprobación o no, sea de la criticidad que fuere.
  Por supuesto hay cambios rutinarios y bajos donde este visto bueno será un mero formalismo, pero aunque sea así es aconsejable que este hito de control también pase por su verificación, sobre todo para evitar que esas "rutinas" dejen de ir cobrando importancia hasta que llegue un momento en que la suma de ellas desencadene en algo más grave.
  En nuestra experiencia, la ausencia de seguridad en el control de cambios siempre ha sido uno de los mayores focos de incidentes de seguridad en las empresas, por esta razón es que deseamos hacer hincapié en que este área sea la que en todos los cambios establezca los requisitos de seguridad que apliquen al mismo.

- Identificación del cambio.
  Cualquier área de la organización podrá identificar la necesidad de realización de un cambio para el normal funcionamiento de su trabajo.
  Cuando se identifica esta necesidad, se inicia el proceso de creación de un ticket de solicitud de cambio, empleando la herramienta de ticketing que posea la empresa. Si no se cuenta con alguna plataforma de ticketing, es necesario que se arbitre las medidas para que se pueda dejar el registro completo de todo el proceso.
  El primer paso de la generación de este ticket es la identificación del tipo de cambio que se solicita, los cuáles a título de ejemplo pueden ser: de hardware, a programas, sistemas operativos, aplicaciones, servicios, dispositivos de red, rutas de comunicaciones, reglas de filtrado, etc.
  Cuanto más acotado e identificadas se encuentren estas opciones en el flujo de ticketing, más eficiente será este proceso.

- Actuaciones ante cambios de emergencia.

  Una necesidad real de toda organización es la realización de cambios no programados que pueden surgir por una incidencia provocada o no. Todo administrador de redes y TI seguramente ha sufrido este tipo de problemas en más de una oportunidad.

  Lo importante en estos casos es actuar siempre respetando el flujo establecido. Es probable que en alguna ocasión ocurra que las acciones a llevar a cabo no puedan responder estrictamente al flujo de este procedimiento, llegado este caso, la idea sería respetar en todo lo posible el flujo establecido en el procedimiento con los menores desvíos admisibles y, por supuesto, al finalizar el cambio, iniciar un proceso de inclusión de esta nueva realidad en el flujo del procedimiento.

  Lo importante de este flujo de emergencia, es ofrecer un camino de urgencia en resolución del problema minimizando la posibilidad de que impacte en otras zonas, áreas o infraestructuras.

  Por ello este tipo de flujos de emergencia deben estar contemplados, debe existir una cadena ágil y eficiente de escalado y contactos adecuados en el NOC y SOC para informar inmediatamente su lanzamiento.

  El sistema de ticketing, también debe contemplar esta posibilidad para que se pueda de forma urgente y sencilla, iniciar esta solicitud y lanzar la actividad. Si el flujo y el sistema de ticketing está bien definido, el mismo se irá encargando de generar las alarmas y alertas necesarias, y a su vez comenzará a dejar sentada la secuencia de acciones que se estén realizando.

  En cualquier caso, el responsable de este cambio, deberá competir todo el conjunto de acciones a posteriori, de forma tal que este cambio se acerque lo máximo posible a todos los requerimientos normales del proceso de gestión de cambios, y sobre todo sea cerrado con todas las garantías del mismo.

- Estado del cambio.

  Sobre la base de la evolución del proceso completo del cambio, este se podrá encontrar en uno de los siguientes estados:

  a. Solicitado: se ha iniciado el ticket correspondiente.

b. Aprobado: Ha pasado por el comité de cambios y ya posee su visto bueno.
c. No aprobado (o rechazado): Ha pasado por el comité de cambios y no posee su visto bueno.
d. Aplazado: Ha sido aprobado, pero está pendiente de ventanas o recursos (físicos, económicos, humanos o temporales) para su lanzamiento.
e. Reprogramado: Se ha iniciado y no se logró completar en su totalidad (o debió sufrir un rollback). Se asigna una nueva fecha para su continuación.
f. Planificado: se ha superado esta fase, pero aún no se ha lanzado.
g. Cerrado: Se realizó y finalizó de forma satisfactoria.
h. Reabierto: Un cambio que ya había sido cerrado, se vuelve a abrir para alguna mejora, o solución de aspectos no conformes.

- Clasificación.

Es lógico pensar que no todos los cambios son iguales. Dependiendo del tipo de cambio que se realice debe establecerse al manos la siguiente clasificación:

- Tipo de cambio:
  a. Programado: Son los que cuentan con todo el proceso de planificación y responden al flujo completo de cambios.
  b. Emergencia: Son cambios que deben realizarse sin seguir el flujo normal, y se deben a razones de urgencia para solucionar algún desperfecto, necesidad imprevista, o incidencia y, que de no ser ejecutados de forma perentoria ponen en peligro la disponibilidad o el normal funcionamiento de las redes y/o sistemas de TI.
  c. Mantenimiento preventivo: Asegura o preserva el nivel alcanzado en la infraestructura.
  d. Mantenimiento correctivo: Resolución de un fallo detectado.
  e. Legislativo: Adaptación a alguna nueva regulación.
  f. Nueva implementación: Incorporación de nuevas funcionalidades, hardware o software a la infraestructura actual.

- Criticidad:
  El flujo de cualquier tipo de cambios, estará regido por la criticidad que debe ser asignado al mismo. Esta criticidad deberá responder al menos a las siguientes categorías:
  a. Baja: muy baja probabilidad de afectación.
  b. Media: Existe un bajo riesgo y potencialmente puede afectar un área acotada de la organización.
  c. Alta: Pone en riesgo áreas importantes de la organización, su impacto de negocio es considerable.
  d. Crítica: Cualquier fallo ocasiona un alto impacto en la organización. El cambio implica infraestructuras críticas del negocio.

- Registro.
  El proceso de registro de cambios, debe ser una parte importante del sistema de ticketing. En todo el flujo descrito anteriormente deberá quedar el registro de las acciones, herramientas, actores y documentos empleados en todo el proceso. Deberá tener la posibilidad de referenciarlo a cualquier otro ticket que guarde relación, como así también a los dispositivos, URLs, rutas, áreas, etc. que participaron o formaron parte del mismo.
  Otro factor a considerar con estos registros es el período de almacenamiento e historial de los mismos, cuya duración deberá depender de cada empresa, pero aconsejamos que nos sea inferior a un par de años.

- Evaluación de impactos potenciales.
  Cuando la organización ha realizado un buen **análisis de riesgo**, tema desarrollado en capítulos anteriores, recordemos que la Identificación, cuantificación y valoración de activos son pasos clave del mismo y a su vez si consideramos que la "Inter relación entre los mismos" es el paso que sigue, cuando es hora de realizar un cambio, si fuimos haciendo las cosas bien, resultará muy sencillo identificar qué otros recursos guardan relación con los del foco del cambio. El riesgo ya lo sabemos de cada uno de ellos, por lo que el impacto potencial que puedo

ocasionar este cambio será muy sencillo de estimar. Nuevamente reflexionemos en lo importante que es haber sido meticuloso con este tipo de trabajos, pues una vez más estamos viendo cómo se concatenan uno a otro.

- Definición de responsables.

  En uno de los primeros puntos de este capítulo, ya se han definido los perfiles de responsables que se deben considerar en el proceso de gestión de cambios. En ese punto es donde se deben presentar de forma concreta (con nombre apellido y contacto) los responsables que participarán en cada uno de los cambios a realizarse, que por supuesto gran parte de ellos serán diferentes en cada cambio.

- Planificación del cambio.

  La planificación del cambio, una vez aprobado o de acuerdo al flujo correspondiente debe realizarse teniendo en cuenta al menos lo siguiente:

  a. Determinación del momento óptimo del cambio.
  b. Análisis de períodos de "freeze" de áreas, plataformas o segmentos de red.
  c. Inicio de la Actividad (preparación, notificaciones, alertas, pruebas).
  d. Validación de pruebas.
  e. Inicio de Implementación (Definición de ventanas de trabajo, si son necesarias)..
  f. Secuencia de Implementación detallada.
  g. Medidas a adoptar en caso de prolongarse el cambio.
  h. Responsables, intervinientes y contactos.
  i. Definición y explicación del punto crítico para continuar con la actividad o realizar regresión del cambio (rollback).
  j. Medidas extraordinarias si es necesario detener el cambio.
  k. Ejecución del cambio.
  l. Ejecución de rollback, en caso de ser necesario.
  m. Monitorización y supervisión del cambio.
  n. Pruebas de validación finales.
  o. Fin de Actividad.
  p. Reportes, actualizaciones y registros.

- Procedimiento de marcha atrás (rollback).
  Esta parte del proceso es fundamental y jamás debe ser dejada de lado. No se trata únicamente de contar con los últimos backups de los dispositivos involucrados en el cambio, sino también de la práctica previa de su funcionamiento e implementación. Cuando el proceso de cambio tiene un impacto relevante, se recomienda la realización de pruebas y tests previos en maquetas o reproducción que garanticen que la vuelta atrás es eficiente en tiempo y forma, sin generar fallos y cumpla con el tiempo necesario asignado o evaluado.

- Plan de pruebas.
  El plan de pruebas, muchas veces es el gran olvidado de esta película, pero cuando se trata de cambios de alto coste e impacto no puede ser dejado de lado. No estamos diciendo aquí la prueba en concreto, sino la planificación detallada sobre la ejecución de esa prueba.
  Como experiencia, hemos visto en muchas oportunidades la ejecución de cambios cuyo coste era millonario, en los cuáles las pruebas de maquetas no eran todo lo detalladas que debían ser o, peor aún, no se contaba con la maqueta necesaria (pues esos dispositivos eran de altísimo coste) y por esta razón se encargaba al proveedor la ejecución de una prueba del cambio en sus propias maquetas. Nos ha sucedido, en la vida real, y con cambios millonarios, que luego de haber realizado la prueba en la maqueta del proveedor y pagando un considerable coste por la prueba en su maqueta, habiendo recibido en visto bueno del proveedor, luego, en el momento de la ejecución del cambio en producción ocurrieron fallos que implicaron la vuelta atrás (en más de una oportunidad…). Al retomar el tema con el proveedor y evaluar las causas, no se podían deslindar con claridad las responsabilidades sobre este proceso, pues no había sido claro el "plan de pruebas" no los detalles técnicos de la imagen, arquitectura, implementación, actualizaciones, interfaces, interconexiones, periféricos, componentes de hardware, etc. Cuando se está trabajando con cambios de alto coste, este plan de pruebas debe ser todo lo detallado que sea

posible, para evitar dejar el mas mínimo parámetro de lado que pueda ocasionar un fallo, luego, en el cambio real en producción.

- Empleo de maquetas y pre-producción.
  Como acabamos de mencionar, siempre es aconsejable la realización de pruebas previas en entornos diferentes al de producción. En muchos casos, es muy sencillo montar maquetas que sean verdaderos "espejos" de lo implantado en producción, laboratorios o entornos en pre-producción.
  Hoy en día con la facilidad que nos ofrecen los entornos virtuales, este tipo de implementaciones, la mayoría de las veces están a nuestro alcance y debemos tomarlo como una obligación en nuestro trabajo de cambios.
  Cuando no esté a nuestro alcance, recordemos el párrafo anterior, pues nuestros proveedores seguramente sí lo tienen, pero recordemos escribir un "plan de pruebas" detallado, antes de solicitar su empleo.

- Ejecución del cambio.
  La ejecución del cambio es el paso crítico de este proceso, y se inicia cuando se lanza la actividad hasta que se genera el cierre correspondiente. Si se ha implantado y ajustado poco a poco un riguroso procedimiento e gestión de cambios, se habrá minimizado considerablemente el riesgo de esta actividad.

- Evaluaciones de cambio.
  Se trata de la revisión de lo implementado y su consideración de satisfactorio o no. Es responsabilidad del gestor del cambio y básicamente deberá evaluar si:
  - Se desarrollo de acuerdo a lo planificado.
  - Cumplió con los objetivos.
  - Los usuarios o clientes están de acuerdo con el cambio.
  - No se han detectado afecciones colaterales.
  - La supervisión y monitorización se encuentra con parámetros normales de funcionamiento, respecto a antes y después del cambio.

- Paso a producción del cambio.

Como todo sistema físico, un vez realizado un cambio se debe esperar un cierto "régimen temporal" de funcionamiento cuya duración dependerá del cambio y la infraestructura, y luego entrará paulatinamente en el "régimen permanente" de funcionamiento volviendo a su normalidad. Si se ha realizado un buen trabajo, las medidas de supervisión y monitorización, estarán en capacidad de ofrecernos una visión muy eficiente de estos regímenes, con lo que el cierre del cambio y su consideración de estado nuevamente en producción, serán muy fáciles de definir. Lo importante aquí es tener en cuenta que una vez considerado este hito, las medidas adicionales y excepcionales puestas sobre el cambio, también volverán a la normalidad, por lo que si sufre un desvío anómalo en su funcionamiento, será más difícil de detectar si ya hemos cerrado el cambio, con lo que es un hito de especial interés a considerar.

- Bitácoras de cambios.

  La bitácora de cambios es la secuencia completa que se desarrolla durante cada cambio en concreto. Como hemos mencionado, un sistema de ticketing, debe incorporar toda la potencia para obtener el máximo detalle de la misma.

  La importancia de contar con una buena bitácora de cambios, con campos que faciliten su búsqueda y retro alimenten la información de cambios, es que la experiencia que se va obteniendo en cada uno de ellos, buena o mala, se puede volver a aplicar en los cambios futuros mejorando todo el proceso.

- Actualización de documentación posterior al cambio.

  Independientemente del sistema de ticketing, a su vez, en general todo cambio genera actualizaciones y modificaciones en mapas, inventarios y documentación de configuración, a veces también en la organización, jerarquía y áreas de la empresa.

  Si al realizar un cambio, toda esta documentación no queda actualizada, generará inconsistencias en la infraestructura.

  Desde el punto de vista de seguridad, muchas veces nos ha sucedido que se dejan abiertas brechas de seguridad pues no se actualizó este tipo de información, y su consecuencia posterior fueron agujeros en reglas de firewall, mezcla de zonas de

diferente criticidad, roles o perfiles de usuarios incorrectos, mapas e inventarios que no reflejan lo real, etc.

- Mantenimiento del control de versiones.
  Tanto el sistema de ticketing, como toda la información de la organización, si no tiene un claro control de versiones, genera inconsistencia en el acceso a la misma. Retomando un poco el tema anterior, si luego de un cambio, se actualiza la información, tal cual se mencionó en el párrafo precedente, pero luego existen diferentes repositorios o acceso a diferentes versiones de la misma, seguramente habrá personas que accedan a uno y otras a otra, con lo que a la hora de implementar medidas posteriores, nuevamente podemos caer en el problema de abrir o encontrar brechas de seguridad, dependiendo de la versión que hayamos considerando u obtenido. Con esto se desea remarcar la importancia de que estos cambios queden documentados con un robusto sistema de gestión de versionado.

12.9. Control de accesos.

En este capítulo nos referiremos únicamente al concepto de "control de acceso lógico", pues cabe mencionar que otro aspecto que no debe ser dejado de lado es el control de acceso físico, que no será tratado aquí y cualquiera que desee profundizar sobre el mismo, aconsejamos como referencia la norma **UNE-EN 60839** "Sistemas electrónicos de control de accesos".

Antes de comenzar a desarrollar este procedimiento, deseo poner de manifiesto una vez más dos conceptos clave, pues a veces o se confunden, o no se aplica su diferenciación adecuadamente :

- Autenticación: Verificar que es quien dice ser.
- Control de Acceso: garantizar que solo accede donde debe.

Es decir, primero se debe tener en cuenta una robusta metodología de autenticación, una vez que se reconoció al usuario, es necesario canalizarlo a las zonas que le corresponden, ni más, pero tampoco menos de las que debe acceder. En esta tarea es muy importante considerar cuatro conceptos más:

- Usuario: Se debería tratar como una metodología de identificación, que solo valida o no de forma binaria. Es importante presentarlo de esta forma, pues es así como podemos ser rigurosos con la diferencia entre este concepto y los que siguen.

  Debemos considerar aquí qué tipos de usuarios permitimos, o inclusive en su misma nomenclatura que nos permita identificar ciertas características del mismo, por ejemplo:

  - Nominales: u-314, a-527, GTPROE1200, TEL_A_32...
  - Genéricos: cisco, admin, juniper, oracle, operador, alumno... (*debe minimizarse su empleo al máximo*).
  - Sistema: root, administrador, dbadmin... (*debe controlarse y monitorizar su empleo al máximo*)
  - Empleado: empresa.nombre.apellido, nombre.apellido, x.apellido1.apellido2

- Externo: empresa.nombre.apellido.ext, ext-nombre.apellido, x.apellido1.apellido2-ext...
- Anónimo: anonymous.

Es decir, en esta definición nos basamos únicamente en el concepto de "autenticación", es o no es quien dice ser, y nada más. Si somos rigurosos en esta idea, podremos aplicar un muy buen control de accesos sobre la base de las definiciones que se presentan a continuación.

- Grupos: Compuesto de dos o más usuarios. Se suele definir también como conjunto de usuarios con visibilidad entre ellos (*departamento, cliente, empresa, proveedor, cursos, investigación, etc.*).
- Perfiles: Nivel de permisos, áreas o cargos. (*gerente, director, operador, soporte, etc*.).
- Roles: Conjunto de privilegios que se poseen, actividad que realiza ese usuario y/o perfil. Un usuario o perfil puede tener varios roles (*administrador, root, propietario, gestor, auditor, webmaster, analista, editor, writer, creator, monitor, viewer, usuario, miembro, etc.).*

Este procedimiento debe definir claramente los criterios y mecanismos de acceso a las redes y sistemas de TI de la organización. Toda gestión de accesos, como parte del conjunto de gestión documental, debe formar parte del ciclo de vida de la seguridad, por lo que uno de los aspectos más importantes de este procedimiento deberá estar basado en el flujo de control de accesos, el cuál va desde la solicitud de un acceso hasta la revocación del mismo, pasando por cada uno de los responsables y las revisiones que sean necesarias. Los requisitos mínimos que se deben considerar son:

- Inicio de una solicitud.

  Se debe procurar el empleo de plataformas que permitan realizar toda la trazabilidad de la gestión de accesos, desde el

inicio mismo, dejando huella de todo el ciclo de vida de una cuenta, por ejemplo empleo de plataformas de ticketing, evitan el empleo de mecanismos que no lo hacen, como puede ser el correo electrónico, formularios en papel u otros.

Como herramienta Open Source, nuestra recomendación es "**Request-Tracker**" que puede descargarse y emplearse gratuitamente desde: https://bestpractical.com/request-tracker.

Es el sistema de Gestión de Tickets Open Source más empleado. Se trata de un desarrollado en Perl que emplea Apache como servidor Web y una base de datos que puede ser: MySql, Postgres o SQLite. Se integra muy fácilmente con el sistema de correo electrónico que usemos para relacionarlo en el sistema de ticketing y con ello justamente evitar lo que comentamos en el párrafo anterior.

- Flujo de aprobación de un acceso y responsables involucrados en el alta, baja y modificación.

  Para que un acceso a cualquier sistema, host, plataforma o infraestructura sea autorizado debe responder a un flujo preestablecido, con la participación de los actores necesarios para ello, y que en general no debería ser inferior a dos. La norma a seguir debería ser que el responsable directo de ese usuario lo solicite, pase por las diferentes áreas involucradas, hasta llegar al "propietario" del activo, que será el último responsable de aprobación del acceso.

  En el caso de tratarse de usuarios que necesiten altos privilegios, el área de seguridad *siempre* debería formar parte del flujo con carácter mandatorio sobre el mismo.

- Segregación de funciones para evitar conflictos de interés en la asignación de roles.

  La gestión de accesos es uno de los procedimientos donde mas aplica la idea de ser "juez y parte" del mismo. Es decir, no puede suceder que quien gestione un acceso, sea el mismo

responsable y propietario del activo, pues en esos casos, puede ocurrir que por razones de facilidad en la operación, se pasen por alto importantes medidas de seguridad. Este fallo en la seguridad de redes y sistemas suele presentarse a menudo en las áreas de ingeniería, planificación y/o operación, las cuáles controlan el día a día de las redes y sistemas y tienen máximos privilegios sobre ellos, ocurriendo que para facilitar la operación creen accesos temporales, reglas o rutas hacia los mismos, sin seguir un protocolo estricto. El resultado de estas acciones ponen en peligro la seguridad global de la organización, por lo que la segregación de funciones, en un flujo estricto debería ser uno de las mayores aspectos a considerar de este procedimiento.

- Definición de tipos de usuario, grupos, roles y perfiles.

  Siguiendo en línea con la clasificación que hicimos al principio de este capítulo, en este procedimiento debería quedar muy clara la definición de estos cuatro conceptos, tratando de ser lo más específico y detallado en la definición de los que aplican en nuestra organización.

- Ciclo de vida de una acceso.

  Todo acceso debe tener definido un ciclo de vida concreto, no pudiendo crear acceso que no tengan fin. En este ciclo de vida, la clave para por planificar hitos anuales de análisis, revisión y verificación de la totalidad de los mismos, y de ser posible en todos los accesos que se soliciten incluir en el flujo del ticket, una fecha de vencimiento, minimizando al máximo los qu Eno lo tengan.

- Control de cambios (de áreas de trabajo, privilegios, empleo de ventanas, incorporaciones o bajas de personal, accesos temporales).

  El cambio de cualquier categoría de un usuario, de forma automática debería lanzar una revisión de sus accesos. Uno de los factores de envejecimiento precoz de un sistema de control

de accesos, son los cambios internos del personal dentro de una empresa. Los ejemplos son ampliamente conocidos, cuando un programador del área de recursos humanos pasa a formar parte de la plantilla de marketing, o un operador asciende a gerente, o un empleado de ventas, se incorpora al aérea financiera, etc. Cualquiera de estos cambios seguramente modifique los accesos anteriores y cree nuevos accesos.

Si no se tiene sincronizado el sistema de control de accesos con el sistema de recursos humanos, con el directorio activo, el sistema de autenticación o inclusive con el financiero (que sabe al detalle a quién, dónde y que are pertenece el pago), es probable que estos movimientos de personal, ocasionen debilidades en los accesos. Por supuesto que mucho más aún si no se controla el alta y baja de empleados o los contratos temporales.

Cualquier fallo en el control de accesos ante estos dinámicos cambios de la empresa, ocasionará tarde o temprano brechas de seguridad.

- Revisiones periódicas.

  La forma de poder detectar este tipo de brechas que acabamos de mencionar, es por medio de estas revisiones periódicas, las cuáles deberían al menos ser realizadas:

  - Por parte de los propietarios de los activos.
  - Por parte del área de seguridad.
  - Por parte del área de auditoría.
  - Cuando se produzcan cambios.

- Requisitos de inicio de sesión.

  Cuando un usuario que está dado de alta en nuestra empresa o no, desea acceder a cualquier activo, deben tenerse en cuenta al menos las siguientes medidas dentro de este procedimiento:

  - Descripción detallada de controles que aplican

- Prohibición de acceso con cuentas genéricas o de máximo privilegios (se debería forzar el empleo de mecanismos robustos de escalado de privilegios, una vez validados como usuarios nominales con privilegios mínimos).
- Mecanismos de control de escalado de privilegios en sesiones establecidas.
- No difusión de información por parte del sistema ante accesos exitosos o no.
- Presentación de la información mínima en las pantallas de autenticación y acceso.
- Empleo de banners previos y posteriores al inicio de sesión, para dejar claro lo permitido y lo no permitido.
- No visualización de contraseñas en la pantalla de autenticación.
- Límite de acceso ante intentos fallidos.
- Una vez validado, presentación por pantalla del último acceso satisfactorio de ese usuario.

Mantenimiento de las sesiones:

No debería permitirse que un usuario que haya accedido a un activo, pueda permanecer en él el tiempo que desee, por lo que en este procedimiento debería definirse e implantarse al menos:

- Establecimiento de tiempo máximo de sesiones (puede ser diferente por cada rol).
- Establecimiento de un tiempo de cierre de sesión ante inactividad.
- Mecanismos de control y alarmas de sesiones establecidas.
- Empleo de mecanismos de filtrado y restricciones sobre redes e interfaces sobre las que se permite el acceso o no.

- Sistema de control y monitorización de accesos.

  Todo tipo de accesos, como se ha mencionado, debería dejar trazabilidad, por lo que una vez que un usuario intenta validarse en cualquier elemento, automáticamente se tendría que comenzar la generación de Logs, sea válido, o fallido el mismo.

  Esta trazabilidad, debería exportarse hacia un servidor externo de logging, para evitar que ante un incidente, cualquier persona pueda borrar los Logs en local y con ello perder esta trazabilidad.

  Una vez que se desarrolla la gestión de los Logs de acceso, se puede seguir adelante con la trazabilidad de los Logs de operación, es decir los comandos y acciones que ese usuario para que con esto pueda seguirse el rastro detallado de toda la secuencia realizada por este usuario.

  El máximo objetivo de este tipo de sistemas de control es la generación de alarmas ante comportamientos anómalos. Este tipo de medidas son sencillas de aplicar cuando se tiene un conocimiento acabado del comportamiento de nuestras redes y sistemas. No se trata de algo complicado de implementar si se inicia el proceso de forma paulatina, por ejemplo comenzando con la generación de alarmas en conexiones fuera de horarios habituales, fines de semana, accesos cuya duración sea llamativa, usuarios que se validan simultáneamente en dos dispositivos deferentes, que generan más de un salto entre un dispositivo y otro, etc. Es decir, la propuesta es comenzar con esta metodología de gestión de alarmas, con parámetros sencillos, para poco a poco ir ajustando la estrategia.

- Requisitos de privacidad de datos personales acordes a la legislación vigente y en sintonía con los procedimientos que la empresa posea sobre el tema.

  En este punto, se debe considerar especialmente dos cosas:

  - El control de accesos, guarda relación directa con los datos de ese usuario, es decir, que estamos tratando con datos personales. Cada rol o perfil, nos da información del área a

la que pertenece, el nivel jerárquico y hasta sus titulaciones. En muchos casos es necesario incluir sus teléfonos, correos y hasta dirección física donde ubicarlo fuera de la oficina.

- Muchos de los roles de acceso, permiten a su vez visualizar datos personales de las bases de datos o ficheros que cuenta nuestra empresa de clientes, proveedores, usuarios, cuentas bancarias, datos de saludo, financieros, etc. Es decir, muchos de esto roles a su vez, tienen la potestad de acceder a datos personales que no son los suyos.

Hacemos especial hincapié en estos dos aspectos, pues cualquier fallo en ellos, es potencialmente un problema grave de protección de datos personales para nuestra organización y, dependiendo de la legislación del país que estemos puede llegar a ser muy serio el tema.

- Sincronizaciones con otros sistemas de autenticación o control de accesos.

  La integridad del dato, como todos sabemos, es una de las bases de seguridad y lo venimos remarcando desde principios del libro. Cuando un usuario necesita poseer diferentes cuentas, contraseñas y metodologías de acceso dentro de la empresa, es natural que empiece buscar mecanismos de simplificarse la vida, cuestión que va directamente relacionada con una futura brecha de seguridad.

  En la actualidad los sistemas de "Single Sign On" nos facilitan la tarea de unificar justamente usuarios roles y perfiles, para que una vez autenticado el usuario dentro de la empresa, pueda desplazarse a cada sitio a los cuáles nuestro sistema de gestión de accesos le haya permitido con mucha flexibilidad y sin tener la necesidad de recordar (o apuntarse en un papel o post it) la lista de usuarios y contraseñas de cada host al que acceda.

- Obligaciones del usuario.

Todo usuario que que acceda a nuestras redes y sistemas debe conocer al detalle que puede y no puede hacer, para lo cual es necesario describir en este procedimiento, al menos lo siguiente:

- Responsabilidades de las acciones que realice con su identificador de usuario.
- Confidencialidad en el empleo de sus credenciales.
- Prohibición de reproducción de su cuenta y contraseña en cualquier tipo de medio (papel o electrónico).
- No empleo de estas claves e identificadores en otras infraestructuras o plataforma externas.
- Comunicación de cualquier incidente de seguridad con su cuenta de usuario.

- Política de contraseñas.

El empleo de las contraseñas debe quedar claro para todo usuario de la organización, para ello, en este procedimiento debemos tener en cuenta al menos los siguientes aspectos:

- Envío seguro de las mismas.
- Centralización de contraseñas externo (servidores de autenticación tipo LDAP, Kerberos, TACACS, RADIUS, etc.).
- Tamaño y empleo de caracteres especiales.
- Forzado al cambio.
- Duración de las contraseñas.
- Histórico de cambios.
- Auditorías de fortaleza de las mismas.
- Mecanismos de almacenamiento y algoritmos sobre las mismas.
- Prohibición de almacenamiento en texto plano.
- Mecanismos de uso de contraseñas de sistema y aplicaciones automatizadas.
- Empleo de claves simétricas, asimétricas y certificados.

- Empleo de doble factor de autenticación para cuentas de administración.
- Empleo de tokens (algo que tiene física o virtualmente), biometría (algo que caracteriza físicamente), o algo que el usuario sepa hacer (teclado, vocalización de un texto).

- Control de acceso a cuentas privilegiadas.

  Una cuenta privilegiada es toda aquella cuenta que tiene la capacidad de ocasionar incidentes de seguridad, tanto por error no voluntario, como intencionadamente. Sobre este tipo de cuenta debemos incorporar y documentar medidas adicionales que nos permitan:

  - Minimizar accesos privilegiados.
  - Garantizar la trazabilidad de las mismas.
  - Exportar trazas de Logs de acceso.
  - Mecanismos de expiración de acceso.
  - Medidas adicionales de revisión y auditoría de las mismas.
  - Eliminación de toda cuenta por defecto o pre configuradas en todo nuevo sistema.
  - De ser posible, empleo de One time Password (OTP).

- Control de acceso a redes.

  El acceso a los diferentes segmentos de la red de nuestras organización, necesita ser tratado de manera particular, pues como se ha dicho, por ellas circula toda la información de la empresa, que es nuestro bien más preciado. Hay un conjunto de medidas de control de acceso que aplican de forma particular a nuestras redes, y que debemos documentar en este procedimiento:

  - Empleo de filtros, reglas o listas de control de acceso que garanticen la segregación de las mismas.

- Empleo de filtros, reglas o listas de control de acceso que garanticen que únicamente desde ciertos roles o rangos de direccionamiento se accede a cada segmento de red.
- Control estricto de puertos de gestión que imposibiliten los accesos desde segmentos no autorizados.
- Control estricto de acceso desde plataformas de gestión o gestoras (OSS: Operation Support System).
- Empleo de redes o ubicaciones físicas para los accesos de gestión.
- Empleo de plataformas de control de acceso.

Control de acceso al código fuente.

La alteración del código fuente, es uno de los mayores objetivos de un intruso, y cuanto más tiempo puede pasar sin ser descubierto en este tipo de modificaciones, mayor será el compromiso de nuestra empresa, por lo que el control de acceso al mismo es otro de los aspectos sobre los que al menos deberíamos considerar lo siguiente:

- Mecanismos de control de acceso al código fuente.
- Restricciones de permisos sobre directorios.
- Medidas de integridad y control de cambios sobre código fuente.

12.10. Entrada en Producción.

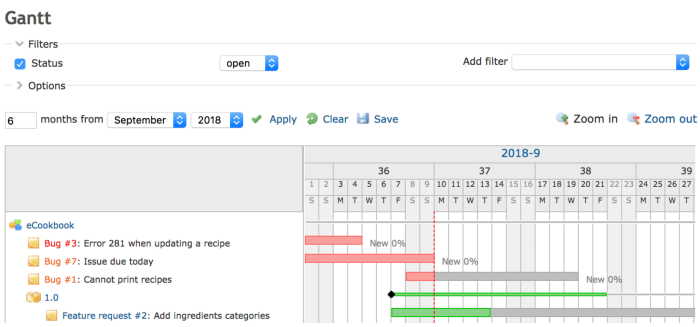
El concepto de entrada en producción implica el conjunto de tareas desde que se propone un nuevo hardware o software, hasta que el mismo se considera que se encuentra en régimen permanente de trabajo, en algunas empresas también se denomina "**creación de planta**".

Como todo administrador de redes y sistemas conoce bien, cualquier modificación a lo que ya funciona implica un riesgo, la importancia de este proceso es justamente minimizar todo lo posible este riesgo, por lo que la redacción y el cumplimiento detallado de este documento es de sumo interés para cualquier empresa. Bajo el enfoque de "resiliencia", motivo de este libro, cuando una infraestructura de ciberseguridad ha alcanzado un cierto umbral, la incorporación de nuevos servicios, por supuesto que modifica ese nivel alcanzado, por lo que en este procedimiento se deberá velar y garantizar que el mismo no se degrade.

Básicamente este proceso nace con una nueva idea que puede surgir por diferentes causas:

- Nuevas necesidades tecnológicas.
- Nuevas necesidades de mercado.
- Nuevas líneas de la empresa.
- Necesidades de migración y/o actualización.
- Propuestas de empleados, proveedores o clientes.

Esta idea, si se aprecia necesario, se plasmará en un proyecto, análisis de viabilidad o conceptualización de la idea. En la actualidad, es común encontrar en las empresas el área de "**oficina de proyectos**" cuya finalidad es justamente la organización y seguimiento del flujo de todo proyecto dentro de la empresa. Existen varias metodologías para esta actividad, El **PERT** (Program Evaluation and Review Technique), el **CPM** (Critical Path Method) o **Gantt**, son actualmente los métodos de programación de proyectos



más utilizados, aconsejamos que por más pequeña que sea la empresa en estas situaciones se apliquen este tipo de metodologías, exista una oficina de proyectos o no. Tenemos a disposición algunas herramientas muy útiles para esta actividad como pueden ser:

Redmine: https://www.redmine.org

Trac: https://trac.edgewall.org

Si la idea o propuesta resulta aprobada, se inicia el proceso de entrada en producción. Los pasos iniciales, dependerán de la magnitud de la empresa y de esta nueva implantación, pero independientemente de si existen licitaciones, solicitudes de compra o presupuestos, convocatoria de proveedores, etc. Los aspectos de seguridad de esta nueva implantación deben ser considerados en un conjunto de especificaciones técnicas o pliegos, en los que el área de seguridad debe participar de forma mandatoria y establecer requisitos de forma previa a la adquisición de productos, con la finalidad de poder evaluar si la futura adquisición cumple con estos requisitos, o no. Este será el primer documento parcial.

Este análisis previo a la compra por parte de seguridad es fundamental, pues en muchos casos no se tiene en cuenta y luego al comenzar las configuraciones, se detecta que no cumple con las funcionalidades necesarias y ya es tarde para revertirlo. Ejemplos de este tipo existen muchos, por ejemplo cuando un elemento no permite o no soporta la configuración de las últimas versiones de un protocolo, como pueden ser **SNMP_v3** (Simple Network Monitor Protocol versión 3) o **NTP_v4** (Network Time Protocol versión 4), estas versiones admiten parámetros de autenticación, confidencialidad e integridad que las anteriores no, y si se ha adquirido un dispositivo que no soporta las mismas, estamos incorporándolo a nuestras infraestructuras introduciendo un punto débil en las mismas. En el caso de sistemas operativos, aplicaciones o servicios es similar, pues es ampliamente conocido que algunas versiones de este tipo de licencias, presentan vulnerabilidades que para ser solucionadas, deben actualizarse con el pago correspondiente de estas.

Este análisis va dando forma a la definición y planificación de cómo se implantará en nuestra empresa este nuevo hardware o software. Aquí es donde ya se empieza a considerar el ciclo de vida de este nuevo elemento, teniendo en cuenta los conceptos de existencia de mercado, costes, compra, soporte, mantenimiento, provisión, recursos, tiempos, plazos, funcionalidades, prestaciones, etc. Cuanto más nivel de detalle se ponga en estos factores, se estará minimizando el riesgo de todo el proceso.

Esta secuencia de pasos ya se puede definir como "**plan de proyecto**" en el que se va definiendo la secuencia de acciones y pasos a seguir. Este plan debe ser revisado y aprobado por la dirección.

En general, se intentará siempre la realización de pruebas de maqueta, como etapa previa a la incorporación de ese nuevo elemento en la infraestructura de producción, para lo cual es necesaria la elaboración de un plan de pruebas, en el que se especifiquen claramente los pasos a seguir, las pruebas y mediciones a realizar, y los resultados esperados. Esta fase formará parte de la certificación de esta nueva implementación, la cual deberá ser aprobada y firmada por los responsables de las áreas de planificación, ingeniería, operación y seguridad.

Si la fase de maqueta resulta satisfactoria, recién ahora se podrá comenzar a planificar y ejecutar las pruebas en un entorno de producción.

Una tarea básica y necesaria antes de comenzar a trabajar en producción con esta nueva implantación es el análisis y la elaboración de un "**Plan de contingencia**", haciendo especial hincapié en la evaluación de los potenciales riesgos que puede implicar incorporar este nuevo hardware o software en la infraestructura. Este plan deberá ser sencillo, eficiente y rápido de aplicar, de forma tal que cualquier fallo o anomalía que se genere puede ser velozmente solucionada, sin impactar el normal funcionamiento de la planta instalada, y por supuesto contemplando el proceso de vuelta atrás.

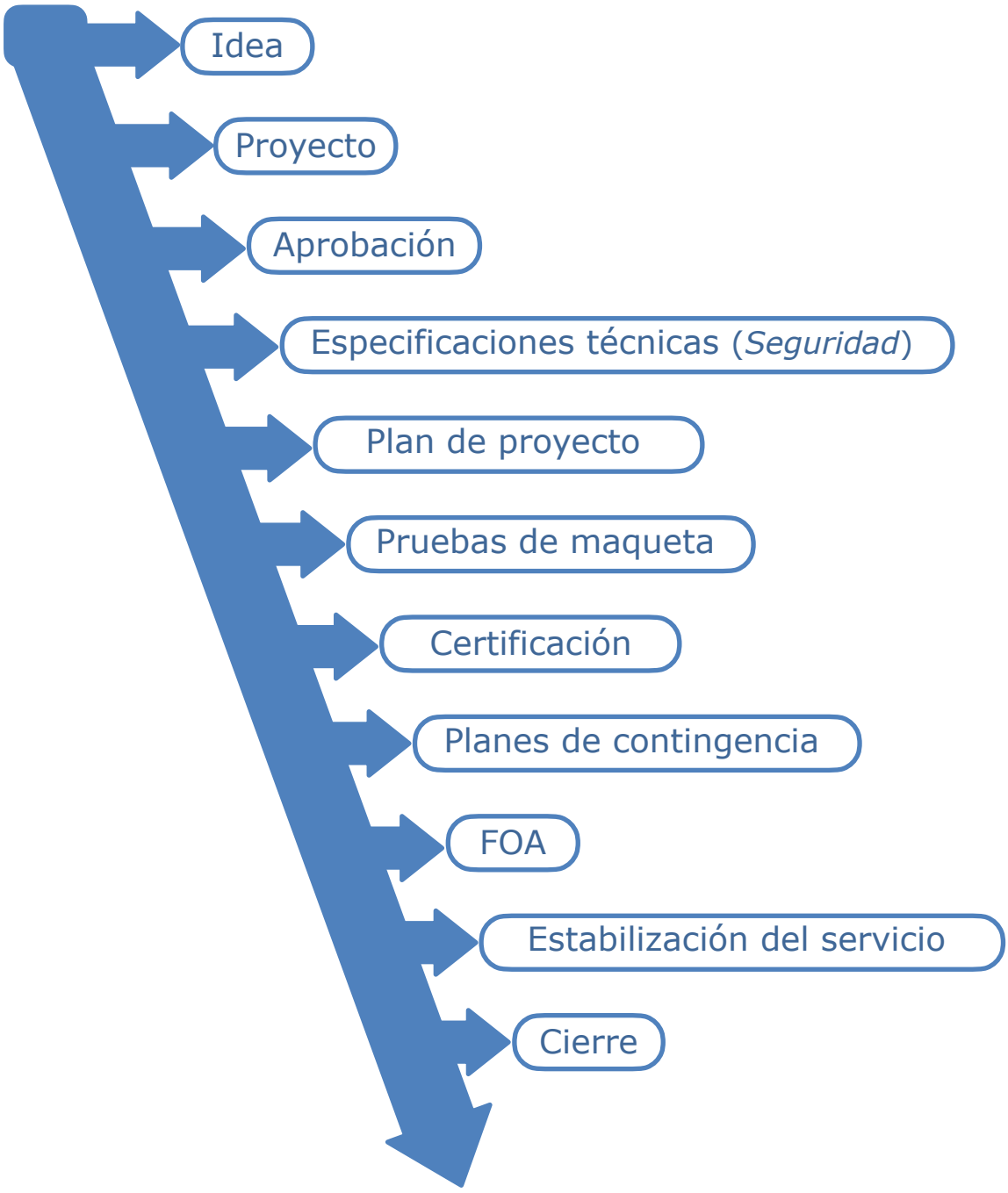
Esta etapa aún no implica un paso definitivo, pues se encuentra en un estado previo a la explotación. La diferencia entre este estado y el de maqueta, es que ahora sobre esta nueva implantación, se analizará su comportamiento bajo un tráfico y funcionalidades reales de este entorno que podríamos llamar "pre producción". Aquí es donde ya podremos observar si su comportamiento es el que se ha planificado y si responde a las exigencias concretas que se han previsto. Esta etapa es, tal vez, la más crítica, pues

acabamos de integrar este nuevo elemento a la infraestructura real, y cualquier fallo puede impactar en nuestros servicios, por lo que se debe centrar especialmente la atención en la programación de acciones y en particular sobre la supervisión y monitorización de toda la infraestructura. Recordemos una vez más la importancia que tiene desde el punto de vista de la resiliencia, el hecho de conocer el comportamiento normal de nuestras redes y sistemas, pues en este tipo de situaciones (y por supuesto también en incidentes) es cuando de verdad es necesario detectar de forma inmediata cualquier desvío del mismo. Este tipo de pruebas previas a la entrada en producción, suele llamarse **FOA** (First Office Application).

Durante esta etapa final se deberá ser muy exigente en el concepto de "**estabilización del servicio**", es decir qué parámetros se considerarán para verificar y asegurar que nos encontramos en un régimen permanente, dejando atrás el concepto de régimen transitorio. No estamos hablando aquí de subjetividades, sino de indicadores y métricas concretas que permitan cuantificar la medición, para que las áreas de supervisión y monitorización puedan dar su visto bueno. Por ejemplo: porcentajes de uso de memoria, CPU, red, tramas o paquetes por segundo, peticiones y respuestas, transacciones, balanceo de carga, bloqueos, etc.

Una vez que se ha estabilizado el servicio, sobre la base de los indicadores definidos, se considera que el hardware o software nuevo ha entrado en producción y se deberá cerrar este proceso. Como consideración final, se debe tener en cuenta que, al haber entrado en régimen permanente, deben quedar incorporados y sincronizados todos sus parámetros con las plataformas de gestión, supervisión y monitorización correspondientes (SNMP, NTP, Gestión de usuarios, gestión de accesos, Gestión de Logs, NOC, SOC, etc.).

El resumen gráfico del flujo que acabamos de desarrollar sería el siguiente:


Idea
Proyecto
Aprobación
Especificaciones técnicas (*Seguridad*)
Plan de proyecto
Pruebas de maqueta
Certificación
Planes de contingencia
FOA
Estabilización del servicio
Cierre

12.11. Seguridad en la comunicaciones.

Tal como venimos insistiendo desde el principio del libro, por nuestras redes y sistemas de comunicaciones circula toda la información de la empresa, por lo que cualquier debilidad en las mismas, es un punto de fuga crítico.

La seguridad de las telecomunicaciones debe ser considerada desde el diseño mismo, teniendo en cuenta varios factores que desarrollaremos en este capítulo y, en particular, tomando como punto de partida el concepto de "prohibición por defecto"

Las redes de telecomunicaciones de nuestra empresa, en líneas generales deben interconectar básicamente:

- Servicios de voz fija.
- Servicios de voz móvil.
- Servicios de datos.
- Áreas internas de la empresa.
- Conectividad con clientes.
- Conectividad con proveedores o partners.
- Conectividad anónima (ej: Internet).
- Ubicaciones físicas fijas.
- Ubicaciones físicas móviles.

Si consideramos estos tipos de conectividad, luego debemos comenzar a definir en detalle que cada uno de ellos, se deberá hacer circular diferentes tipos de información, desde datos triviales hasta la más crítica de nuestra organización, por lo que es necesario seguir avanzando sobre la organización de estos tipos de tráfico, para que nuestra infraestructura de telecomunicaciones nos permita segregar o segmentar cada una de estas áreas y su nivel de criticidad de la forma más eficiente, y sobre todo, "flexible" pues será esta última característica la que nos permitirá mantener a lo largo del tiempo los umbrales de seguridad planteados.

Un procedimiento de gestión de redes, debe considerar al menos los siguientes aspectos:

- Seguridad desde el diseño.

  Se debe describir el conjunto de acciones previas a evaluar y realizar desde el momento mismo que una nueva necesidad de red se pone de manifiesto.

- Capacidad de la red.

  Cada segmento de red debe ser dimensionado para el uso al que se le dará. No es lo mismo un acceso a una base de datos que consolida la totalidad de la información del negocio de la empresa y que tramita millones de transacciones por segundo, que el servidor de mensajería y la red de gestión fuera de banda. Cada uno de estos servicios, necesitará un ancho de banda diferente, y el diseño de la arquitectura de una u otra puede hacernos ahorrar o malgastar enormes cantidades de dinero, o lo que es peor, ralentizar todo el funcionamiento de la empresa.

  La capacidad de una red, es un factor de diseño clave que luego es muy difícil y costoso de revertir si ha sido mal calculado o poco expandible en su diseño. Si se posee experiencia y buen historial sobre nuestra infraestructura de telecomunicaciones, es sumamente sencillo de dimensionar, el problema suele estar con nuevos desafíos. La facilidad, ancho de banda y abaratamiento de costes que hoy en día nos ofrece la fibra óptica, es una gran ayuda en los casos que podamos realizar nuestros propios cableados, pero el problema aquí está en las ubicaciones distantes en las que nos encontramos ante la necesidad de contratar estos vínculos a terceros, los que suelen ser de un coste considerable, y por esta razón es una muy buena medida saber considerar que flujo de información circulará por los mismos para evitar pecar por exceso o por defecto.

Una sigla que suele ser bastante representativa que también debemos tener en cuenta en el diseño de la capacidad de una red, es **RMA** (Reliability, Maintainability, y Availability) que en español se traduce como confiabilidad, mantenibilidad (o mantenimiento) y disponibilidad.

En muchos casos, y en general dependiendo de la magnitud de la empresa o la red, se deben considerar aspectos como los de alta disponibilidad para garantizar la disponibilidad y confiabilidad, y también el balanceo de carga, donde a través del empleo de diferentes tipos de hardware o software, puede distribuirse el flujo de datos entre más de un camino y servidor, descongestionando el rendimiento.

- Seguridad por niveles.

El modelo de capas TCP/IP propone los cuatro primeros niveles para actividades de red, dejando el nivel de aplicación (quinto nivel). Cuando se diseña la seguridad de una arquitectura de red, se deben considerar los cuatro primeros niveles:

- En el nivel físico hay que tener en cuenta la seguridad del cableado y de la ubicación de los dispositivos de red.
- El nivel de enlace, suele estar bastante olvidado, pero recordemos que dentro de entornos LAN y a nivel WiFi es clave y existen un sinnúmero de ataques de spoofing, arp, icmp, etc. que no requieren gran complejidad. En este nivel se deben tener en cuenta las diferentes recomendaciones de IEEE, por ejemplo: 802.1x, 802.1q, 802.11i, etc.
- El nivel de red es fundamental en cuanto al empleo de rutas dinámicas o estáticas, de protocolos de enrutado que permitan seguridad OSPF, BGP, EIGRP, etc. Prestar especial atención a la elección de los rangos de red y subred por medio de direccionamiento IPv4 privado y público, aplicando listas de control de acceso. En el caso de emplear IPv6 se debe tener en cuenta también los rangos auto asignados, y la convivencia con IPv4.

- En el nivel de transporte, lo primero a prestar atención es al empleo de protocolos no orientados a la conexión (UDP: User Datagram Protocol) u orientados a la conexión, que en este último caso existen TCP (Transport Control Protocol) y hoy ya está vigente SCTP (Strem CTP) que ofrece mecanismos de seguridad más robustos. Este nivel es uno de los más exigentes en el empleo de FWs, y en particular, sobre lo que acabamos de mencionar de los protocolos orientados a la conexión, pues una funcionalidad típica de estos dispositivos es el "control de estados" que nos permite cubrir una amplia gama de ataques de tipo gota a gota, sesiones abiertas, cierre de sesiones, detección de IDSs, etc.

- Prohibición por defecto.

La mejor forma de describir esta concepto es, justamente, apelando a los firewalls que acabamos de mencionar. Cuando se diseña una arquitectura de firewalls, existen dos metodologías:

- Holgadas: Se permite todo, y se va cerrando poco a poco.
- Ajustadas: Se niega todo y se va abriendo poco a poco.

Si hemos comprendido la lógica de lo que los dos párrafos anteriores, ahora podemos relacionarlo con nuestras infraestructuras, pues es muy difícil, en una red que lleva años funcionando y con gran dispersión de funciones y/o servicios, comenzar cerrando todo, pues seguramente paralicemos la empresa, por el contrario, en una arquitectura reciente, es muy sencillo hacerlo, pues a medida que entran en producción nuevos servicios, se van abriendo las rutas y puertos que se necesiten.

Como cabe esperar, es muchísimo más seguro, comenzar con todo cerrado, es decir: prohibición por defecto, pero por supuesto este principio no será válido de aplicar de forma radical y de un día para el otro, en una empresa que lleva años sin considerar esta idea.

Lo importante aquí es quedarnos con el concepto, y no dudar en que es fundamental a considerar, el cómo hacerlo, ahí sí, dependerá de la arquitectura que tengamos.

- Fallo seguro.

En este caso, también me gusta iniciar poniendo por ejemplo un dispositivo muy útil a la hora de trabajar con IDSs, que se denomina "splitter" o "tap". Se trata de una hardware que tiene cuatro conectores físicos (de fibra óptica y/o cable UTP), dos de ellos, se emplean para cortocircuitar el segmento de red real, es decir, se coloca interceptando todo el tráfico que circula por ese cable, los otro dos, son por los que "espeja" el tráfico entrante y saliente de los dos conectores anteriores. Estos dispositivos, como cabe esperar, son de suma utilidad porque en estos dos últimos conectores es donde se conecta nuestro sistema de detección de intrusiones, el cual de forma totalmente transparente permite analizar el 100% de tráfico que circula por este segmento de red, y diferenciarlo en un sentido u otro. La característica fundamental que tiene este hardware, es que se trata de un dispositivo "normal cerrado", lo que implica que si se produce cualquier tipo de fallo en el mismo (por ejemplo ausencia de alimentación), los dos conectores iniciales de entrada y salida real de nuestra red, seguirán funcionando como si el tap no existiera, evitando con ello, cualquier tipo de fallo.

En el caso de las redes, esta característica de diseño es también fundamental, y no solo ante fallos técnicos, sino también ante fallos intencionados, como por ejemplo un intento de interceptación. Si en algún momento, alguien desconecta un cable y conecta un dispositivo, o también lo hace conectando su ordenador a una boca de un switch o router, en primer lugar sería deseable que la red lo detectara, y en segundo lugar también sería importante considerar la posibilidad que por más que lo haga, no pueda hacer uso de la red. Cualquiera de estas opciones, hoy en día está soportada por medio de medidas de seguridad, como pueden ser los protocolos de nivel de enlace mencionados: IEEE 802.1x, como también por medio de la no

asignación de dirección IP, el dejar "down" los puertos no activos, con mecanismos de autenticación robustos o por medio del empleo de diferentes opciones criptográficas.

- Control de acceso a la red.

  Ya se han desarrollado algunos conceptos al respecto, pero lo importante ahora, más allá de los mecanismos y medidas que adoptemos es tener claro que existen dos tipos de control de acceso a una red: el control de acceso físico y el lógico. Siempre deben ser analizados ambos tipos y por supuesto aplicadas las medidas oportunas, dependiendo de la criticidad de la red a la que estemos accediendo.

- Segregación de redes.

  El concepto de segregación de redes, es básicamente la separación de las mismas. El nivel de seguridad que hayamos decidido darle a un dispositivo, servicio o función, en principio dependerá del grado de segregación de las redes que tengamos. Es decir para acceder a un servicio, deberé haber podido circular por las redes adecuadas que me permitan legar hasta el mismo, una vez llegado al punto de destino, existirán medidas de control de acceso o no hacia ese servicio, pero la ruta que se siga para llegar hasta él, dependerá de lo que hayamos permitido o no ir "saltando" entre los diferentes segmentos de red.

En grandes redes, u organizaciones complejas, es una muy buena práctica contar con un procedimiento específico que regule la segregación de estas redes, y el conjunto de medidas y permisos que se aplicarán entre ellas.

Hace varios años, publiqué un artículo que se llamaba "**Matriz de estado de seguridad**" que puede descargarse gratuitamente en:https://darfe.es/es/nuevas-descargas/category/4-tec en el mismo se presentan diferentes fórmulas y cálculos que, a título de ejemplo, pueden ser tenidos en cuenta

para desarrollar zonas y parametrizar los diferentes valores de cada una de ellas, a la hora de segregar redes.

- Redes inalámbricas.

  El mito de la seguridad en redes inalámbricas ha pasado de moda, hoy la familia IEEE-802.11i, nos ofrece mecanismos y algoritmos tan seguros como cualquier red cableada, el tema pasa por emplearlos de forma adecuada y considerando especialmente los segmentos a los cuáles nos permite acceder o no. En los libros anteriores ya hemos desarrollado bastante sobre este tema, pero lo que queremos destacar aquí es la importancia de tener en cuenta este tema y procedimentarlo con todo el detalle que haga falta.

- Acceso desde redes externas.

  Lo que consideramos red interna, es la que interconecta toda la infraestructura de nuestra organización, teniendo en cuenta cada uno de los conceptos que hemos ido desarrollando, asociada a los niveles de seguridad de sus segmentos y los permisos de acceso de cada grupo rol o perfil.

  En la actualidad, el concepto de movilidad es una de las realidades de toda empresa, es necesario habilitar mecanismos para que el personal pueda acceder a los servicios de la organización esté donde esté. Este tipo de accesos externos a la infraestructura tiene que tener la capacidad de diferenciar el rol o perfil de quien se haga presente para dirigirlo a los recursos que tenga asignados. Este conjunto de mecanismos y controles son los que debe ser redactados en el procedimiento.

- Cableado de las redes.

  El cableado de toda infraestructura de red debe responder al concepto de cableado estructurado, tema que queda regulado con todo detalle por la norma TIA/EIA 568 y ha sido desarrollado en los libros anteriores.

Aspectos que no pueden faltar en este punto son los que desarrollen:

- Normas de etiquetado de la empresa.
- Normativa de ductos y subductos.
- Procedimientos de conectorizado.
- Certificaciones de cables, fibras y medios de transmisión inalámbrica.
- Protección de extremos y terminadores.
- Puntos de inspección.
- Empleo de armarios o racks de comunicaciones.
- Empleo del cableado en zonas públicas.
- Tendidos aéreos.
- Protecciones electromagnéticas, de humedad y temperatura, apantallamientos, y guías de cableado.

- Protección física del cableado y dispositivos de red.

En este procedimiento deben especificarse el conjunto de medidas físicas que se deben considerar para los ductos que porten el cableado de la red, como así también las ubicaciones de los diferentes dispositivos.

- Bastionado de dispositivos de red.

Cada dispositivo de red deberá contar con las respectivas guías de bastionado, y las mismas deberían a su vez contemplar las versiones más actuales de cada uno de ellos.

Sobre las guías de bastionado, creemos que dos grandes referentes son:

guías **CIS**: CIS Center for Internet Security®

https://www.cisecurity.org/cis-benchmarks/

guías del **CCN-CERT** de España:

https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

- Dispositivos de protección de redes.

  Dentro del procedimiento deben considerarse también el conjunto de dispositivos que la empresa tiene implantados o planifica implantar, con los detalles de sus funciones y prestaciones. Sobre cada uno de ellos, deberá quedar claro en qué ámbito aplica y cuáles son las normas de configuración de todo elemento que se integre a la red respecto a los mismos. Este tipo de dispositivos, en general serán: firewalls, servidores de tiempo, servidores de autenticación tipo RADIUS o TACACS, servidores de Logs, servidores de monitorización y supervisión, sistemas de detección o prevención de intrusiones, sistemas AntiDDoS, sistemas de centralización de antivirus y parcheado, sistemas de gestión de red (OSSs), etc.

  Este tipo de dispositivos son críticos dentro de la arquitectura de red, por lo que su empleo y parametrización no puede quedar sujeta a ambigüedades, en particular respecto a cada componente de la red, por lo que cuando entra en servicio, o sufre un cambio cualquiera de ellos, las consideraciones sobre todos estos dispositivos deben ser foco de especial atención.

- Monitorización y supervisión.

  Toda arquitectura de red debe contar siempre con herramientas y/o plataformas que realicen esta actividad, pues son los ojos de la red. Dependiendo de la magnitud de la red, tendrá mayor o menor cantidad de recursos asignados, pero aunque sean mínimos los mismos, debe existir "sí o sí" esta

actividad, debiendo documentarse con el máximo detalle en este procedimiento.

Para esta actividad existen cientos de soluciones, una mejor que otra, es difícil poder decidir cuál es la óptima, pero a continuación mencionamos algunas de ellas que creemos están bien posicionadas y son de las más difundidas:

PRTG Network Monitor:

https://www.paessler.com/prtg?gclid=EAIaIQobChMI55j_2MH86wIVU4jVCh0AqQ0AEAAYASAAEgJBF_D_BwE

Nagios XI: es uno de los software de supervisión de redes más potente y fiable del mercado.

https://www.nagios.com

OpenNMS:

https://www.opennms.com

Infoblox:

https://www.infoblox.com

Solarwinds:

https://www.solarwinds.com/es/free-tools/real-time-netflow-analyzer

Zabbix:

https://www.zabbix.com

Splunk Enterprise:

https://www.splunk.com

IPSentry:

https://www.ipsentry.com

SentinelAgent:

https://www.sentinelagent.com

EventSentry:

https://www.eventsentry.com/4.1

Icinga:

https://icinga.com

Kentik:

https://www.kentik.com

PulseWay:

https://www.pulseway.com

- Voz sobre IP.

  El concepto y las aplicaciones de voz sobre IP ya son una realidad, tanto en entornos LAN como WAN, en llamadas internas como externas nacionales e internacionales. Si nuestra organización posee cualquier tipo de infraestructura que aplique este tipo de tecnologías, debe ser documentada debidamente.

  Hemos detectado muchas debilidades y puertas traseras a través del empleo de dispositivos y redes de voz sobre IP. En varias empresas, este tipo de redes no están segregadas del resto de la arquitectura IP, ni implementan mecanismos robustos de seguridad, por lo que los teléfonos, centrales e infraestructuras de señalización (que emplean los protocolos **SIP**, **SDP** y **RTP**) tienen visibilidad hacia toda la red de la organización, teniendo en cuenta que un teléfono IP hoy en día posee toda la capacidad de un ordenador estándar, por lo que al haber comprometido cualquiera de ellos, ya se está operando desde dentro de la empresa. También existe una amplia variedad de herramientas de hacking y secuestro de llamadas que facilita todo tipo de actividad maliciosa, partiendo desde la escucha e interceptación de llamadas, hasta el robo de puertos y saltos dentro de la arquitectura de red.

  En resumen, cuando en una empresa se implanta cualquier tipo de medidas de voz sobre IP, debe considerarse su estrategia de seguridad como cualquier otro dispositivo o red IP.

- Uso correcto de las redes.

  Cada perfil o rol dentro de la empresa, sus proveedores, partners y clientes, deben conocer al detalle sus responsabilidades y obligaciones en el uso de las redes. Una muy buena práctica es incorporar un apartado de estos temas en la política de seguridad de obligado cumplimiento que deberá estar firmada por toda persona a la que se le de acceso a las mismas. Con esta medida, se garantiza el debido tratamiento de cualquier mal uso de la misma, inclusive ante la necesidad de apelar ante instancias judiciales.

El uso indebido de una red de telecomunicaciones, puede ocasionar perjuicios dentro y fuera del ámbito de la organización, por esta razón es que es vital prestar interés en la redacción de esta parte del procedimiento.

- Documentación de las redes.

Ese punto deberá ser uno de los más importantes a redactar y mantener actualizado en nuestras redes. Una adecuada documentación de red nos asegurará la prevención, detección y tratamiento correctos ante cualquier incidente o anomalía, como así también nos facilitará la tarea de su expansión o modificación, tema que es extremadamente dinámico hoy en día. Se desarrollará por medio de diagramas o mapas, teniendo en cuenta los niveles de la red como así también los flujos que sustenta. Deberá incluir el detalle de las configuraciones de sus dispositivos, como así también los repositorios principales, secundarios y de resguardo de toda esta información.

Se debería prestar especial atención a la metodología de mantenimiento y actualización de todo el ciclo de vida de esta documentación.

12.12. Responsabilidades, obligaciones y funciones del personal.

Este procedimiento, deberá definir todo lo que puede o no puede hacer el personal propio o ajeno que ingrese en nuestras instalaciones, redes y sistemas de TI. Jurídicamente es un documento clave, pues todo aquello que se desconoce puede dejar abiertas alegaciones no deseadas, por el contrario, si una persona tiene conocimiento sobre el tema, firma su enterado y luego no lo cumple, la situación difiere substancialmente. Por esta razón, en este procedimiento es una buena práctica la definición de un anexo que acompañará la documentación que firmará todo personal previo a la contratación si es interno, o se incluirá en los contratos con terceros.

El contenido de este documento debería al menos considerar los siguientes aspectos.

- Acceso físico.

  Tanto para usuarios externos, como internos de la empresa deben quedar establecido los permisos que cuenta para acceder a las diferentes instalaciones de la empresa, como así también los mecanismos de autenticación física requeridos (carnet, llave electrónica, biometría, etc.).

  Este punto debe guardar relación con la señalización de las áreas y el conjunto de medidas de control de acceso físico que, independientemente de lo que se regule en este procedimiento, mantendrán a resguardo y restringidas las áreas que así se determinen.

  Un aspecto clave a tener en cuenta, en relación con la protección e datos personales, es que se deberá informar con claridad las áreas o zonas en las que se encuentren cámaras de video vigilancia, con los carteles respectivos que pongan en conocimiento del área que están cubriendo. Dependiendo de la regulación del país, será necesario, o no, que el personal firme su consentimiento a esta actividad.

- Identificadores de usuario y claves de acceso.

  Los empleados no deben comunicar a otra persona, en ningún caso sus credenciales (identificador de usuario o su claves de acceso). Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso debe ponerlo en conocimiento del responsable del sistema, con el fin de que le sea asignada una nueva clave.

- responsabilidades y obligaciones sobre los activos.
  - Auto protección de sus propios activos.
  - Apagado de equipamiento al finalizar sus tareas o jornadas laborales.
  - Comunicación de anomalías
  - Empleo de antivirus.
  - Proteger su identificación y claves de usuario ante difusión a cualquier otra persona.
  - Mantener el nivel de seguridad exigido para la información sensible.
  - Dependiendo de la empresa, se deberán desarrollar aquí también las medidas a tener en cuenta para todo activo que se entregue al personal, de forma temporal o permanente, y los pasos a seguir para su recepción, mantenimiento y devolución.

- Prohibiciones.
  - Destruir, alterar, inutilizar o daños hardware, software o información de la empresa.
  - Obstaculizar intencionadamente el acceso de otros usuarios mediante el uso o consumo abusivo de recursos.
  - Realizar acciones cuyas consecuencias dañen, interrumpan o generen errores en la infraestructura.
  - Escalar, o intentar escalar los privilegios que tiene asignados.

- Intentar distorsionar o falsificar los registros de cualquier sistema.
- Intentar descifrar las claves o algoritmos de cifrado y /o cualquier otro elemento de seguridad implantado en la empresa.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la empresa o de terceros.
- Instalar software no autorizado.
- Efectuar modificaciones de hardware o software en los equipos informáticos sin conocimiento del Responsable de Seguridad y autorizado por éste.
- Cambiar la configuración de los recursos corporativos, tales como el nombre de nodo, la dirección IP, el método de acceso a la red, etc.
- Borrar cualquiera de los programas instalados legalmente así como cualquier fichero que impida o dificulte su normal funcionamiento.
- Difundir o compartir sus claves de usuario.
- Envíos masivos de correos, con fines comerciales o publicitarios, sin el consentimiento explícito de la organización.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o, en general, los archivos de otros usuarios, excepto aquellas personas autorizadas expresamente por la empresa.
- Intentar acceder a áreas restringidas de los sistemas informáticos de la empresa, tanto a nivel físico como a nivel informático.
- Borrar cualquiera de los programas instalados legalmente.

- Utilizar los recursos telemáticos de la empresa, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos mercantiles de la empresa, dentro de la red corporativa puesta a disposición de las actividades corporativas.
- Enviar o reenviar mensajes en cadena o de tipo piramidal.

Confidencialidad de la información.

Todo envío de información clasificada de la empresa al exterior, mediante soportes materiales o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso, debe ser realizado de acuerdo a lo establecido en el procedimiento de "Gestión de de la Información".

Los usuarios de los Sistemas de Información de la organización deben guardar, por tiempo indefinido, la máxima reserva sobre los datos, documentos, metodologías, claves, análisis, programas y demás información, en soporte material o electrónico, a la que tengan acceso durante su relación laboral con la empresa, no pudiendo divulgarlos ni utilizarlos directamente o a través de terceras personas o empresas. Esta obligación se mantendrá vigente tras la extinción del contrato laboral durante el tiempo que estipule la empresa con el trabajador.

En aquellos supuestos en los que un empleado, por motivos directamente relacionados con su puesto de trabajo, entre en posesión de información clasificada en cualquier tipo de soporte, debe entenderse que dicha posesión es estrictamente temporal, con obligación de confidencialidad y sin que ello le de derecho alguno de posesión, titularidad o copia sobre la referida información. El empleado debe devolver dichos materiales a la empresa inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de

forma diferente a la pactada y sin conocimiento de la empresa no supondrá, en ningún caso, una modificación de esta norma.

- Destrucción de soportes.

  Los empleados deben conocer y emplear los medios necesarios para destruir los soportes que contengan información clasificada antes de desecharlos.

- Propiedad intelectual.

  En primer lugar deben establecerse las medidas de propiedad intelectual sobre las licencias y el software que es de propiedad de la organización, prohibiendo el empleo de programas sin su correspondiente licencia.

  En segundo lugar, es muy importante destacar, regular y prohibir el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por los derechos de propiedad intelectual o industrial de la empresa. debe quedar claro contractualmente con el empleado que la propiedad intelectual e industrial de todo desarrollo que desarrolle el mismo, será de la empresa y no del empleado. Esto último ha sido foco de millonarios juicios e incidentes de seguridad por fallos en las obligaciones y responsabilidades de ambas partes en los contratos y toma de conocimiento del personal.

- Incidencias.

  Se debe establecer con claridad las obligaciones del personal sobre cómo debe comunicar a sus responsable cualquier incidencia que se produzca y que tome conocimiento. Dicha comunicación debe realizarse siguiendo lo establecido en el procedimiento de "**Gestión de incidentes**".

  El personal deberá ser consciente que toda investigación de incidentes así como la manipulación de la información que se origine, será realizada siempre por personal autorizado y con

conocimientos técnicos relevantes. Que bajo ningún caso puede iniciar por cuenta propia y sin autorización este tipo de actividad.

- Uso del Correo Electrónico

No será considerado como privado ningún mensaje de correo electrónico dirigido o enviado a través de los servicios informáticos de la empresa puestos a disposición y uso de los empleados, siempre que existan otros métodos de acceso a cuentas de correo privadas a través de la red corporativa o acceso controlado a recursos exteriores. En caso de que no exista acceso a cuentas de correo electrónicas privadas, el correo corporativo se considerará no exclusivamente privado, pero se permitirá dicha funcionalidad. Se considera correo electrónico tanto el interno, entre terminales o usuarios de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, Internet.

Cualquier fichero introducido en la red corporativa o en el equipo informático del usuario a través de mensajes de correo electrónico que provengan de redes externas debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y al control de virus o códigos susceptibles de originar situaciones anómalas en los sistemas informáticos.

- Acceso a Internet

El uso del sistema informático de la empresa para acceder a redes públicas como Internet, se limita a los temas directamente relacionados con la actividad de la empresa y los cometidos del puesto de trabajo del usuario.

El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información, tales como FTP, Chat, IRC y similares, se limita a aquellos que contengan directamente información relacionada con la actividad de la empresa o con los cometidos del puesto de trabajo del usuario.

La empresa, como propietaria de estos recursos puestos a disposición de sus empleados, se reserva el derecho a monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet.

Asimismo, cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y al control de virus o códigos susceptibles de originar situaciones anómalas en los sistemas informáticos.

- Datos de carácter personal.

La privacidad en el tratamiento de los datos personales, internos o externos de la organización, hoy en día es una de las mayores prioridades de toda empresa. De acuerdo a las regulaciones del país, deberá contarse con un procedimiento específico que regule cómo se aplican las medidas dentro de la organización.

Todo el personal de la empresa, deberá recibir formación al respecto y evaluar los resultados del conocimiento adquirido, desarrollando programas de formación que garanticen el claro conocimiento del tema por todo el personal contratado (interno y externo).

En este punto se deberá desarrollar especialmente el acceso que puede o no tener cada empleado a los datos de carácter personal que almacena y procesa nuestra empresa, bajo el principio de necesidad de conocer y en función de las responsabilidades, roles y perfiles de cada empleado o puesto de trabajo.

Se deberá garantizar que únicamente acceden a estos datos o ficheros las personal autorizadas, y de acuerdo a la sensibilidad del dato concreto, se deberán arbitrar todas las medidas necesarias para dejar registrado estos accesos, como así también toda actividad que la persona realice sobre el dato.

La violación de cualquiera de estos aspectos relacionado con los datos personales debería tener un nivel de infracción grave dando lugar a la aplicación de severas sanciones.

Una muy buena referencia a la hora de informarse y obtener guías de buenas prácticas sobre este tema es la Agencia Española de Protección de Datos: https://www.aepd.es/es

- Penalizaciones.

El personal deberá conocer y se consciente de los procedimientos de penalización que posee la organización ante los diferentes tipos de incumplimiento de las obligaciones del personal, como así también la evasión de responsabilidades.

Todo procedimiento sancionador deberá responder a las legislaciones del país, y prestar especial atención a la secuencia adecuada de pasos y evidencias a incluir, dejando documentada de la forma que la ley lo establezca cada paso realizado.

En general un procedimiento sancionador, se puede lanzar por las siguientes vías:

- De oficio: Algún superior en la jerarquía de ese empleado, tiene fundadas sospechas que esa persona ha cometido una infracción.
- A instancia de partes interesadas: Se presenta una denuncia verbal o escrita de algún trabajador.
- A instancia de partes externas: Se presenta una denuncia verbal o escrita de alguna persona externa de la empresa, proveedor, partner, cliente o inclusive se debe contemplar, o no, la posibilidad que sea iniciado de forma anónima.

Se deberá establecer aquí una escala de infracciones, con niveles que generalmente suelen considerar desde muy grave, grave y leve. Para cada uno de ellos se debería establecer con claridad, y de ser posible con máximo detalle, los casos en los

que aplica y el tipo de sanciones que se pueden aplicar en cada caso.

Finalmente, es muy importante también, dejar claros los plazos de cada uno de estos pasos o fases, para que no pueda existir la posibilidad legal que se cometan errores de procedimiento.

12.13. Gestión de terceros (proveedores, partners y clientes).

La gestión de terceros, será el proceso que nos permita delimitar obligaciones y responsabilidades con todo personal externo a nuestra organización. Se trata de una pieza clave para toda empresa, pues de la relación con los mismos dependerá la subsistencia de toda empresa. Desde el punto de vista de la seguridad hay varios aspectos que deben ser tenidos en cuenta.

En el caso de los partners o proveedores el objetivo de este documento es el de proteger la información y los activos que manejan, o con los que tratan los mismos, y garantizar la seguridad de toda la empresa.

Toda externalización de un servicio pueden suponer una ventaja operativa pero por supuesto será un nievo riesgo que deberá se analizado, implementando nuevo las medidas y controles adicionales que surjan de este análisis.

- Determinación de las obligaciones regulatorias, legales, gubernamentales, contractuales y comerciales, así como de la normativa interna aplicables.

  En términos generales, lo que se presenta aquí son los acuerdos de nivel de servicio, o más conocidos como SLA (Service Level Agreement) que deberán describir de forma concreta, al menos los siguiente puntos:

  - Alcance del servicio o producto.
  - Nivel de criticidad.
  - fechas de inicio y fin del contrato.
  - Horario en el que se realizará el servicio, soporte o trabajo.
  - Canales de comunicación e interlocutores.
  - Tiempos máximos de respuesta.
  - Requisitos específicos del producto o servicio.
  - Máximos tiempos de fallo, cortes o ausencias.

- Política de reposición de recursos (materiales o humanos).
- Facilidades y restricciones de acceso a los entornos contratados.
- Procedimientos y documentación que se exigirá al proveedor.
- Autorizaciones para verificar la veracidad de la información ofrecida por el tercero.
- Calendario de revisión del SLA.

Derecho a ser auditado.

Todo personal o empresa externa deberá aceptar poder ser auditado en los términos, responsabilidades y obligaciones que formen parte del contrato, como así también en sus instalaciones y procesos al tratarse de empresas, si esta auditoría fuera necesaria para la evaluación de los términos del contrato.

Tratamiento de la información por parte del tercero.

Toda la información a la que el tercero tenga y de acuerdo a su nivel de clasificación, deberá ser evaluada previamente al contrato, para poder determinar con la mayor precisión posible, las medidas que se aplicarán y los niveles de acceso que se le asignará al tercero, que podrán ser similares, o no, a los del personal interno.

Acceso del tercero a activos de la empresa.

El propietario de cada activo de la empresa será el responsable de determinar los controles de acceso que se deben aplicar a terceros. El área de seguridad deberá participar y supervisar las medidas que se adopten.

Contractualmente deberá quedar reguladas as obligaciones y responsabilidades del tercero respecto a los activos a los que se le permita acceder, dejando claro que será éste el responsable de las actuaciones que pudieran dar lugar a sanciones y/o multas que por tales infracciones puedan ser imputadas a la empresa, como así también por los daños y perjuicios que se deriven del

incumplimiento sobre el uso adecuado del activo, resarciendo a la empresa por los importes que hubieran tenido lugar, incluyendo gastos jurídicos, extrajudiciales y costes adicionales.

- Tratamiento de datos personales.

  En la terminología de la Unión Europea, toda persona que accede a datos personales a los que un "responsable del dato" le haya permitido acceder pasa a ser "responsable del tratamiento". Sobre este tema, el proveedor deberá adoptar las medidas técnicas y organizativas que garanticen que cumple con un nivel de seguridad similar al de nuestra empresa, y firmar el contrato de tratamiento correspondiente. El formato de este tipo de contratos puede encontrarse como modelo en la Agencia Española de Protección de Datos: https://www.aepd.es/es

- Definición de los niveles de servicio y necesidades de soporte exigibles al proveedor.

  Los niveles de servicio a los que se comprometa el proveedor deberán quedar claramente reflejados en el contrato, pues este suele ser uno de los factores más importantes desde el punto de vista de resiliencia. El grado de respuesta, apoyo o soporte que brinde el proveedor, será una de las herramientas más importantes con la que cuente nuestra empresa, por esa razón, en particular en situaciones críticas, no puede prestarse a ambigüedades, dudas o demoras.

- Desarrollo específico de un conjunto de especificaciones de seguridad, para la solicitud de información y ofertas por parte de los proveedores.

  Siempre que se considere la contratación de algún servicio o artículo por parte de un proveedor, las especificaciones técnicas sobre aspectos relativos a seguridad deberá ser un apartado a tener en cuenta. Cuanto mayor detalle se ponga en las mismas, menores serán los riesgos asociados en el futuro contrato.

- Evaluaciones sobre capacidad técnica de la empresa y los recursos que asigne el tercero.

  En la actualidad, con el volumen de información presente en Internet, es muy sencillo poder obtener antecedentes y proyectos en los que haya participado una empresa. A su vez existen certificaciones y organismos que avalan la trayectoria de cualquier organización. Cuando se presente la necesidad de contratar algún producto o servicio a un tercero, su evaluación técnica, previa a l contrato debería ser una de las medidas básicas a adoptar.

  Una realidad muy presente a la hora de contratar personal externo, es que la empresa prestadora de este servicio, presenta perfiles genéricos de los puestos y funciones a cubrir, cuando llega la hora de ejecutar las mismas, esos perfiles genéricos, no cuentan con la formación exacta que se necesita para ese rol o función. Para evitar este tipo de situaciones, se debe prestar especial atención en la descripción de los puestos o funciones que se necesitan, como así también con el perfil y cualificaciones que debe tener el personal que lo cubra. En los casos en que fuera posible, lo ideal es la realización de entrevistas previas con el personal que se incorporará con la capacidad contractual de aceptarlo, o no, si la empresa considera que no se ajusta estrictamente al perfil que se necesita.

- Evaluaciones sobre la especificaciones técnicas de seguridad de los productos y servicios ofrecidos.

  En línea con el punto anterior, el producto o servicio que se va a contratar, debería evaluarse, en primer lugar de forma teórica, analizando sus especificaciones técnicas y prestaciones, y luego de ser posible mediante la realización de pruebas de maqueta, o en entornos de preproducción. Este paso, es también importante por razones de compatibilidad e integración con el resto de la infraestructura, por otro lado permite también analizar si las prestaciones teóricas se corresponden con la realidad y soportan su implementación en un entorno similar al real.

- Regulaciones y mecanismos a aplicar para la transferencia de conocimiento.

Una constante que se suele encontrar a la hora de contrataciones es el problema que se comienza a generar con la dependencia al proveedor, cuando un nuevo producto o servicio entra en producción en la organización. Toda dependencia, nos quita libertad de acción, cosa que jamás debemos perder. En todo contrato, se debe considerar los mecanismos y cláusulas adecuadas para que el conocimiento del proveedor paulatinamente se vaya transfiriendo a la empresa.

- Planes de capacitación.

  La transferencia de conocimiento del punto anterior, de ser posible, debería ser planteada por medio de planes de formación concretos con costes asociados y previstos en el contrato, que permitan ser implantados en el período del contrato y cuyos resultados puedan se medibles de la forma más objetiva posible.

- Certificaciones que pueden ser requeridas.

  Dependiendo del producto o servicio a contratar, hoy en día existen diferentes tipos de certificaciones que deberían ser consideradas como exigencias hacia el proveedor, tanto para la empresa proveedora como así también para el producto o servicio que se vaya a contratar. Este tipo de certificaciones son una garantía de la calidad de lo que se vaya a contratar, por lo que debe ser siempre tenidas en cuenta.

- Monitorización y supervisión de desempeño del tercero.

  Durante el período comprendido por el contrato, deben establecerse las medidas de monitorización y supervisión que aplicará la empresa sobre el proveedor, con la finalidad de evaluar su desempeño y anticiparse a cualquier desvío que pueda ocurrir con la máxima antelación posible.

- Mecanismos de control sobre altas, bajas y modificaciones del personal que asigne.

Los mecanismos de autenticación y control de acceso de la empresa, de ser posible deberían contemplar la posibilidad de integrar en los mismos, cuentas, grupos, roles y perfiles de personal ajeno a la misma. esta capacidad es fundamental en este caso, pues son sumamente peligrosos los fallos en el control de cuentas externas, dejando abiertos accesos, permisos o usuarios que han sido cambiados de puesto o empresa, o proveedores que ya han finalizado su actividad.

En los casos de personal interno, esto suele ser más sencillo de controlar pues el área de recursos humanos y financiera, lleva el control estricto de su personal. Esto no es necesariamente así cuando el personal que interviene no está en la nómina de la organización, por lo que se pueden presentar zonas grises sobre estos usuarios, que no quedan bajo el paraguas de control de estas áreas, ni de seguridad.

Se han presentado un sinnúmero de incidentes de seguridad con este tipo de cuentas, en particular con empleados de empresas externas que han finalizado su contrato, y sus cuentas seguían en estado activo con los privilegios que en su momento se le asignaron, en particular se debe considerar que en muchos casos este tipo de accesos, se realizan en remoto, lo que agrava la situación.

- Mecanismos y métodos concretos para la extinción o recesión de contratos.

Se debe prever en el contrato la posibilidad que la empresa externa no cumpla con las expectativas deseadas o no satisfaga las necesidades del proyecto, producto o servicio. Existen muchos casos, donde el motivo del contrato es fácilmente cuantificable, medible u objetiva; si es así será sencilla la tarea de definir incumplimientos. e no ser así es importante también definir cláusulas que den la libertad de poder finalizar el contrato con este proveedor pues estaría dejando de prestarme los resultados para los que lo contraté. Un problema grave, y muy importante en aspectos de seguridad y sobre todo de resiliencia, es tener que convivir con un proveedor que no cumple con los niveles de servicio o calidad de sus prestaciones.

- Devolución de activos que hayan sido entregados por las partes y destrucción segura de la información intercambiada.

  En el contrato debe quedar claro la entrega y devolución de activos hacia el proveedor, como así también su responsabilidad de cuidado, mantenimiento, seguridad física y lógica de los mismos. En cuanto a la información que trate el tercero, se establecerá la metodología de resguardo, atribuciones sobre la misma, y finalmente los pasos a seguir con ella a la hora de finalización del contrato. En los casos que esta información deba ser borrada, se establecerán los mecanismos para garantizar que se realice de forma segura, dejando constancia por escrito de esta actividad.

- Medidas particulares que minimicen la dependencia con el proveedor.

  Tanto para productos, como para servicios, existen medidas particulares que pueden ser tenidas en cuenta para evitar dependencia con ellos. Ejemplos de esto pueden ser el empleo de estándares de mercado que eviten protocolos o productos propietarios, el empleo de código abierto, la adquisición de hardware certificado por el mercado y compatible con otros fabricantes, el desarrollo de software respetando metodologías reconocidas y exigiendo su documentación detallada, el empleo de algoritmos criptográficos públicos, etc. Este tipo de medidas son muy beneficiosas a considerar contractualmente a la hora de renovar contratos o decidir cambio de proveedores.

- Tribunales a los que recurrir legalmente ante incumplimientos, incidentes o desacuerdos contractuales.

  Se establecerá a qué jurisdicción legal se apelará ante cualquier tipo de demandas por desacuerdos con los términos del contrato.

- Penalizaciones en casos de incumplimientos de contrato.

  Se dejarán establecidas qué tipo de penalizaciones se ponen de común acuerdo, en caso de los diferentes grados de incumplimiento

que pudieran surgir sobre los términos del contrato. Cuanto más claras sean las mismas, menores errores de interpretación se generarán ante desacuerdos.

12.14. Cumplimiento legal.

Este procedimiento, en algunas ocasiones se ha puesto en duda si debe formar parte o no de la resiliencia de una infraestructura de seguridad. Desde nuestro punto de vista es clave en este marco de resiliencia, pues las consecuencias legales de cualquier paso en falso, puede desencadenar en que toda una empresa no logre recuperarse ante cualquier incidente o anomalía en su estrategia de ciberseguridad. Hemos vivido personalmente, situaciones en las que haber respetado estrictamente las medidas de cumplimiento legal, permitieron demostrar de forma contundente las responsabilidades sobre actos vandálicos o incidentes provocados de forma intencionada.

En lo personal, hubo dos grandes casos que para mí fueron muy significativos.

El primero de ellos sucedió hace unos años cuando un empleado, que era administrador de una serie de dispositivos del core de la red de una gran empresa, fue despedido por robo. Tenía instalada una antena específica que permitía acceder desde su casa en forma remota para los casos en que necesitaba su actuación fuera de horario (que nadie conocía…). Con saña y desde su domicilio luego del despido, se dedicó a desconfigurar y borrar los switchs más importantes que eran el core de la organización, pudo hacerlo pues aún tenía máximos privilegios (recordar también el proceso de "Obligaciones y responsabilidades del personal" y el de "Gestión de accesos"). La red quedó fuera de servicio durante veinticuatro horas, la empresa fue multada con treinta y un millones de dólares. cuando se detectó el incidente, de forma inmediata se lanzó el análisis de los hechos y, respetando estrictamente los procesos de gestión de incidentes y cumplimiento legal que se encontraban muy bien implantados, se siguieron todos los pasos de acuerdo a la legislación de ese país, se informó a las autoridades, se llamó un notario para dejar constancia de cada acción, se realizaron todas las copias de resguardo con su hash correspondiente, se logró identificar la antena y los logs que había dejado esta persona, se tomó contacto con el CSIRT de ese país, se solicitó la intervención de las fuerzas de seguridad para el análisis de frecuencia y radio de propagación de esa antena, se identificó su cobertura, y al realizarse una nueva conexión por parte de esta persona, pudo ser identificado legalmente. Ese conjunto de

acciones que cumplían con todo los procedimientos, tuvo como resultado que esta persona sea llevada a juicio, declarada culpable, detenida y la empresa aseguradora tenga que hacerse cargo de la multa. Tal vez algún lector pueda pensar que esto no guarda relación directa con el concepto de resiliencia, si esta es su hipótesis, le propongo que haga números y analice si su propia empresa podría recuperarse en el caso que el seguro no se hiciera cargo y tuviera que desenvolver treinta y un millones de dólares, en mi caso seguramente no me recuperaría (es probable que mis tátara nietos tampoco).

El segundo ejemplo fue similar, pero el fallo no fue intencionado, sino debido a que un empleado de la empresa externa (recordar también el proceso de "gestión de proveedores"), se conectó a las doce horas del mediodía, sin haber solicitado ventanas de trabajo (recordar también el proceso de "gestión de cambios") y detectó que estaba corrupta la base de datos de un nodo importante de la red. Como se trataba de un cluster, el otro servidor seguía funcionando sin inconvenientes, entonces por cuenta propia, decidió recuperar esta BBDD corrupta por medio del servidor que funcionaba bien de este cluster, pero cometió el error de hacerlo en sentido inverso... es decir, recupero la BBDD corrupta sobre la buena. A los pocos segundos, se produjo una avalancha de encolado en otros nodos de la red que soportaban esta función pues, comenzaron a llegarle millones de peticiones adicionales, debido a que el cluster principal estaba caído con ambas BBDD corruptas. El segundo nodo, tenía parámetros muy ajustados sobre el volumen de transacciones a procesar y, ante esta avalancha, se cayó también, sucedió lo mismo con el tercero, el cuarto y así los ocho nodos que prestaban este servicio. La consecuencia fue que la red al completo se cayó. El servicio que prestaba esta empresa facturaba millones a la hora, con lo que cada hora que pasaba eran pérdidas millonarias. El proveedor, aunque aún no se sabía que había sido responsable del hecho, fue informado del incidente, y comenzó a intentar repararlo, puso a once personas simultáneamente a trabajar en esta actividad, cuando uno hacía algo, otro lo deshacía, cuando uno decía "A", el número cuatro decía "X" y el siete "J", cuando uno se conectaba a un nodo a hacer algo, otro se conectaba a otro a hacer otra cosa. Las primeras horas fueron un verdadero caos generalizado, y por supuesto no encontraban el fallo. Así fue durante las siete primeras horas, hasta que la solución fue desactivar unos algoritmos de autenticación que permitieron que todo el mundo (literalmente) se conecte y de esta forma el servicio se levantó pero aún sin

ninguna restricción de acceso, es decir la empresa facturaba a sus clientes, pero los que no lo eran también podían acceder y usar estos servicios de forma gratuita. La identificación del problema real, demoró varias horas mas, y prácticamente se tardó un día más en restablecer todo con normalidad. En el análisis forense, se logró descubrir la causa raíz del fallo, con las evidencias necesarias como para identificar el empleado que la ocasionó. En este caso, no se tuvo que recurrir a los tribunales, pues en virtud del contrato de servicio con este proveedor era evidente que incumplía de varios aspectos, tanto de gestión, como de soporte. El incumplimiento de este contrato, especificaba claramente las penalizaciones y tribunales a los que recurrir en caso de incumplimiento, los SLA estaban bien redactados, con lo que se logró acordar en buenos términos una solución adecuada a las importantes pérdidas sufridas. En este caso, no se tuvo que recurrir a los juzgados, en virtud de tener claro que si se hacía de esta forma, el proveedor sería aún más perjudicado, y todo esto se debió a una muy buena estructura de procedimientos y contemplando los aspectos de cumplimiento legal, de forma que fue indiscutible la asignación de responsabilidades.

Ejemplos de este tipo de buenas y malas prácticas en los procedimientos de cumplimiento legal, existen cientos. El no empleo de "banners" de inicio de sesión ha ocasionado pérdidas en instancias judiciales, pues el intruso adujo que desconocía que estaba accediendo a algo prohibido. La evidencia de un correo electrónico que presenta de forma inequívoca, que un empleado está enviando fuera de la empresa información confidencial, puede quedar desbaratada, si no se le informó al empleado que su correo de empresa puede ser monitorizado y supervisado. El empleo de cámaras de vigilancia en pasillos o zonas seguras de la empresa, puede no ser una evidencia legal, si no existe la cartelería y documentación adecuada. Una escalada de privilegios improcedente, no implica infracción, si la persona no lo ha firmado como indebido, etc.

En resumen, lo que hemos querido transmitir es que un buen procedimiento que define los conceptos de cumplimiento legal y en sintonía con la legislación del país, en nuestra opinión sí impacta en la resiliencia de redes y sistemas de TI.

En este procedimiento, el punto de partida es identificar y establecer los controles necesarios para el cumplimiento legal, regulatorio y contractual, de acuerdo con la tipología de servicio a prestar o contratar.

Este procedimiento debe satisfacer las necesidades de las partes interesadas (personal propio, clientes, proveedores, etc.).

Un procedimiento de cumplimiento legal debería incluir al menos:

- Identificación y análisis de la legislación aplicable.
- Acciones desarrolladas para la adecuación legal vigente.
- Regulaciones sobre controles criptográficos (especial atención a este punto en los países que aplique).
- Mapa de riesgos.
- Medidas para la adopción de decisiones.
- Programa y directivas de prevención penal.
- Modelo de gestión de recursos financieros para impedir delitos.
- Medidas anticorrupción a aplicar en la empresa.
- Obligaciones de reportar a organismos de supervisión y control.
- Sistema de penalizaciones y sanciones.
- Mecanismos de detección y actuación.
- Medidas rectoras de información personal, intimidad y datos sensibles.
- Daños y delitos informáticos.
- Delitos contra la propiedad intelectual e industrial.
- Análisis detallado de la legislación del país, en los artículos que aplican a nuestra empresa.

De los puntos anteriores, quisiéramos explayarnos un poco mas sobre el programa y directivas de prevención penal, pues es parte fundamental de este procedimiento.

Este Programa posee una doble función:

- Evitar que en nombre de la empresa y en su provecho, sean cometidos delitos por sus representantes legales, administradores, responsables de redes o sistemas de TI, o por aquellos que están autorizados para tomar decisiones en nombre de la misma; además, igualmente, que puedan ser

cometidos delitos, en el ejercicio de las actividades sociales y en beneficio directo o indirecto.

- Establecer los mecanismos para que, pese a esta función preventiva, las personas mencionadas cometan delitos, poner éstos de forma inmediata en conocimiento de la autoridad competente, cumpliendo así con el deber de denuncia que establece la legislación vigente.

Si la magnitud de la empresa lo permite, es muy importante contar con una metodología y canal de denuncias, al que tengan accesos, empleados, clientes y proveedores y ofrezca los mecanismos básicos y las garantías para que sea tratada de forma adecuada, cualquiera que se presente.

En esta misma línea de magnitud, se debe incorporar también en este procedimiento los mecanismos y políticas antifraude y anticorrupción, que regulen este tipo de delitos y establezcan pautas claras de conducta a todo el personal de la empresa.

Otro apartado a contemplar también son los delitos de explotación de personas, los cuáles deben regular de forma concreta el conjunto de medidas de protección a los trabajadores de la empresa, incorporando apartados específicos sobre la legislación en materia de discapacidad.

En España, por ejemplo, el Código Penal en su artículo 197.3 define con toda claridad: "*El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años*".

El mismo código penal en su artículo 264.2 también regula que: "*El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años*".

Es decir, si mi empresa está radicada en España y mis empleados van a operar con los sistemas informáticos de la misma, deben haber tomado conocimiento por escrito de estas regulaciones y su penalización, pues de

esta forma, en el caso que cualquiera de ellos la incumpliera, la responsabilidad penal recaería sobre el empleado que cometió el delito. En el caso que mi empresa no se lo haya informado, ni el empleado haya firmado el haber tomado conocimiento de estas regulaciones, tal vez logremos librarnos de esta responsabilidad, o tal vez no, puede ser también que seamos solidarios con el delito, pero ya estaríamos entrando en los supuestos futuros de las decisiones judiciales. Cuando existe un robusto procedimiento de cumplimiento legal y el empleado ha tomado conocimiento fehaciente del mismo, la responsabilidad queda claramente definida.

Para ser aún más gráficos respecto a este procedimiento, tomemos como ejemplo la famosa **LSSI** (Ley de Servicios de la Sociedad de la información) de España, la Ley 34/2002, de 11 de julio, de "**servicios de la sociedad de la información y de comercio electrónico"**, la cual al día de hoy tiene una serie de agregados, actualizaciones y modificaciones, pero a los efectos de este texto nos interesa únicamente tomar como base la misma, para que podamos considerar algunos aspectos que debería contener nuestro procedimiento, si nos tuviéramos que ajustar a la legislación de este país, por supuesto lo mismo deberá ser evaluado en el país en que se encuentre nuestra empresa.

El objeto de esta Ley es la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica. Esta Ley se aplica a los prestadores de servicios de la sociedad de la información, es decir cualquier tipo de servicios que nuestra empresa esté ofreciendo relacionados a "sociedad de la información" está afectado por esta ley. Lease: página Web, bases de datos, publicidad o productos que se compran o venden vía Internet, servicios ofrecidos telemáticamente, etc.

Analicemos algunos de sus artículos:

Artículo 8 Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.

> "*1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los*

vulneran. Los principios a que alude este apartado son los siguientes:

……

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual."

Este artículo puede ser denunciado, por ejemplo ante cualquier fotografía que inocentemente, o no, pueda ser subida a nuestra página Web o servidores de mi empresa. Este tipo de errores, son muy frecuentes de encontrar en empresas, cuando por ejemplo, publicitan un evento, congreso, función, acto, etc. y en los resúmenes, comentarios, videos o fotografías del mismo, se nos pasa por alto algún fotograma donde aparece alguien en silla de ruedas, la imagen de un menor de edad, un gesto que pueda ser interpretado como ofensivo, hasta un crucifico de alguien colgado al cuello, publicidad de un determinado sector de la sociedad, etc.

Por supuesto también en lo que afecta al último párrafo respecto a la propiedad intelectual , donde el empleo de software, artículos, referencias, música de fondo, videos, etc. que tengan el resguardo correspondiente puede ocasionar multas muy cuantiosas o la necesidad de tener que realizar un proceso de vuelta atrás que os costaría importantes recursos.

Orto artículo de esta misma Ley es el **Artículo 10** Información general

"1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

Cualquier ausencia de los datos que nos indica este artículo en nuestros servidores hacia "*los destinatarios del servicio como a los órganos competentes*" puede ocasionar un recurso que desvirtúe un contrato, o cualquier tipo de relación comercial ya cerrada y pactada, con las consecuencias que esto pueda conllevar, por incumplimiento la LSSI.

Por último, el **Artículo 20** Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.

> *"1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.*
>
> *2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.*
>
> *4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo".*

Este artículo de verdad me encanta, pues en Europa ha sido motivo de sanciones de alto impacto en empresas que no lo han cumplido, y seguramente todos nosotros hemos sufrido en carne propia esta violación de la Ley.

El punto clave sobre este último artículo es denominado "publicidad engañosa" y en muchos países ya cuenta con suficiente base regulatoria, como para que se incorpore la misa a esta procedimiento.

El procedimiento debe tener en cuenta de forma especial las medidas regulatorias en la utilización de los medios técnicos de la empresa frente a cualquier tipo de ilícitos de índole sexual o pornográfico en relación con menores, incitación o o provocación a la discriminación, violencia u odio contra personas, razas, credos o naciones.

Por último, en virtud de las consecuencias legales que puede tener el desconocimiento de este procedimiento, es necesario que cada empleado firme dando fe cierta de haberlo leído, y a su vez se cuente con los mecanismos de acceso al mismo y la comunicación de cualquier cambio que se realice sobre este.

12.15. Gestión del ciclo de vida.

Ya hemos puesto de manifiesto que la ciberseguridad no puede ser pensada como algo estático, sino que se tata de un proceso vertiginosamente dinámico. El umbral alcanzado con nuestra estrategia de ciberresiliencia, si lo descuidamos, con la aparición de nuevas amenazas y la evolución de las ya existentes exige que lo mantengamos o mejoremos, pero si lo dejamos de lado envejecerá rápidamente y el esfuerzo realizado se vendrá abajo.

El objetivo de este procedimiento será definir de forma concreta y medible el proceso de mejora continua que nos exige este concepto de ciclo de vida de la seguridad.

Este documento deberá revisarse en función de cambios organizativos, legales o de negocio que se produzcan en cada momento, y con la periodicidad que se establezca en la empresa.

Si seguimos la lógica del libro, hemos podido establecer una estrategia de ciberresiliencia que presentamos a la dirección para que se decante por un plan de acción a dos años, el cual, definirá los mínimos a cumplir bajo nuestra responsabilidad. Según lo que nos indica la norma ISO 27001, nos encontraríamos bien posicionados en la fase "Plan", para continuar con este ciclo debamos ahora describir en este procedimiento de qué forma abordaremos las siguientes: "Do", "Check" y "Act" en este ciclo, al menos bianual que nos hemos propuesto.

En el capítulo 10. "**Ciclo de vida**" se desarrollaron los conceptos que proponen las normas ISO 27001 y 27004 y se puso de manifiesto que el ciclo de vida es el concepto más importante de seguridad a lo largo del tiempo, por lo que si se trata del concepto más importante es necesario desarrollarlo con todo detalle y documentar los pasos y acciones necesarias para que así sea. En ese mismo capítulo se ha mencionado que: Una organización debe describir cómo se ínter relacionan e interactúan el SGSI y las mediciones, desarrollando guías que aseguren, aclaren y documenten esta relación, con todo el detalle posible. En este documento lo que se trata es de documentar como es esta relación y planificarla, en nuestro caso para los próximos dos años.

- Programa de medición de la seguridad.
- Definición de atributos medibles.
- Definición de indicadores.
- Definición de umbrales a alcanzar.
- Modelo de mediciones.
- Desarrollo de las mediciones aplicables.
- Implementación del programa.
- Revisión de mediciones.
- Mejoras.
- Cuadro de mando.

Para poder desarrollar este procedimiento de forma práctica, supongamos que la dirección de mi empresa ha adoptado su decisión y que ha sido seleccionado el plan de acción intermedio que hemos presentado en el capítulo 9. "Estrategias Resilientes en Redes y Sistemas", tomemos como ejemplo el mismo y avancemos sobre este.

Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas				Ajustes/Medición																		700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño			nuevas configuraciones				ajuste reglas			Pruebas funcionam. Planta		1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS													Análisis/presupuestos			Pruebas			Implementación						5.000 €	3		2º año
(7)	Reposición de grandes equipos	Análisis/presupuestos						Plan migración		1ra. Compra/despliegue			Entrada producción (1ra.compra)	NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
(9)	DRP				Análisis			Fase 1			Pruebas			NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año	
																										24.200 €		17.700 €	6.500 €

Como se aprecia en la imagen, hemos puesto el centro de atención en diez tareas:

(1) Determinación de RTO

(2) Determinación de RPO

(3) Determinación de KPIs

(4) Mejoras en IDSs/IPSs

(5) Obsolescencia BBDD y Backups

(6) Mejoras en AntiDDoS

(7) Reposición de grandes equipos

(8) Formación

(9) DRP

(10) SLAs

Desarrollemos con ejemplo práctico sobre los mismos, cada uno de los puntos de este procedimiento.

- Programa de medición de la seguridad.

  Nuestro programa debería tener como punto de partida la planificación del plan de acción a dos años, por lo que las mediciones deberían ajustarse como mínimo a:

  Como se puede apreciar en las dos columnas finales, también se propone realizar revisiones sobre posibles desvíos.

Nº	Actividad	Año 1	Año 2	Hito 1	Hito 2	Hito 3	Hito 4	Des-víos	Des-víos
(1)	Determinación de RTO	30/3		30/3				*30/12*	*30/24*
(2)	Determinación de RPO	30/3		30/3				*30/12*	*30/24*
(3)	Determinación de KPIs	30/6		30/1	30/3	30/6		*30/12*	*30/24*
(4)	Mejoras en IDSs/IPSs		30/24	30/14	30/18	30/21	30/24		
(5)	Obsolescencia BBDD y Backups	30/6		30/2	30/6			*30/12*	*30/24*
(6)	Mejoras en AntiDDoS		30/20	30/14	30/17	30/20		*30/24*	
(7)	Reposición de grandes equipos	30/12		30/3	30/5	30/8	30/12	*30/18*	*30/24*
(8)	Formación	30/11		30/6	30/9	30/11		*30/18*	*30/24*
(9)	DRP	30/11		30/6	30/9	30/11		*30/18*	*30/24*
(10)	SLAs	30/12		30/6	30/12			*30/18*	*30/24*

- Definición de atributos medibles.

  Recordemos que la norma **ISO 27004** nos indica que:

  - Atributo: Propiedad o característica de una "entidad", que puede ser distinguida cuantitativa o

cualitativamente, por una persona o sistema automatizado.

- Entidad: Un objeto (tangible o intangible), que será caracterizado a través de la medición de sus "atributos".
- Indicador: Es una medida que provee una estimación o evaluación de un "atributo" especificado, con respecto a las necesidades de información definidas.

Por lo que comencemos presentando cuáles son nuestras entidades:

- RTO y RPO.
- KPI.
- IDS/IPS.
- BBDD y Backups.
- Mejoras en anti DDoS
- Grandes equipos.
- Formación.
- DRP.
- SLAs.

Ahora, ¿cuáles son las propiedades o características de estas entidades para que podamos distinguirlas en esta medición?

Nº	Entidad	Atributo
(1)	RPO y RTO	Objetivos de recuperación
(2)	KPIs	Indicadores imprescindibles de seguridad
(3)	IDS/IPS	Sistemas de tratamiento de intrusiones.
(4)	BBDD y Backups	Almacenamiento y resguardo de información
(5)	Grandes equipos	Equipamiento cuyo coste supera los 15.000 €
(6)	Mejoras en Anti DDoS	Protección perimetral
(7)	Formación	Capacitación del personal
(8)	DRP	Planes de recuperación.
(9)	SLAs	Acuerdos con proveedores.

- Definición de indicadores.

Los indicadores, quedarían entonces definidos al asignarle el atributo y entidad de cada uno de ellos, tal cual podemos verlo en la siguiente tabla:

Nº	Entidad	Atributo	Indicador
(1)	RPO y RTO	Objetivos de recuperación	Estado de implantación de RPO y RTO en activos críticos.
			Pruebas y verificaciones de recuperación y comportamiento de RPO y RTO.
(2)	KPIs	Indicadores imprescindibles de seguridad	Definición e implantación de KPIs
			Revisión, modificación e incorporación de nuevos KPIs
(3)	IDS/IPS	Sistemas de tratamiento de intrusiones.	Configuración y actualizaciones
			Evolución de falsos positivos y negativos
(4)	BBDD y Backups	Almacenamiento y resguardo de información	Indicadores de obsolescencia
(5)	Grandes equipos	Equipamiento cuyo coste supera los 15.000 €	Implantación de nuevos servidores
			Evaluación de rendimiento
(6)	Mejoras Anti DDoS	Protección perimetral	Grado de implantación
			Implantación y ajuste de umbrales
(7)	Formación	Capacitación del personal	Planificación e impartición de formación
			Medición de resultados
(8)	DRP	Planes de recuperación.	Porcentaje de implantación
			Pruebas y mejoras
(9)	SLAs	Acuerdos con proveedores.	Análisis de contratos y acciones concretas.
			Incorporación de nuevos SLAs

- Definición de umbrales a alcanzar.

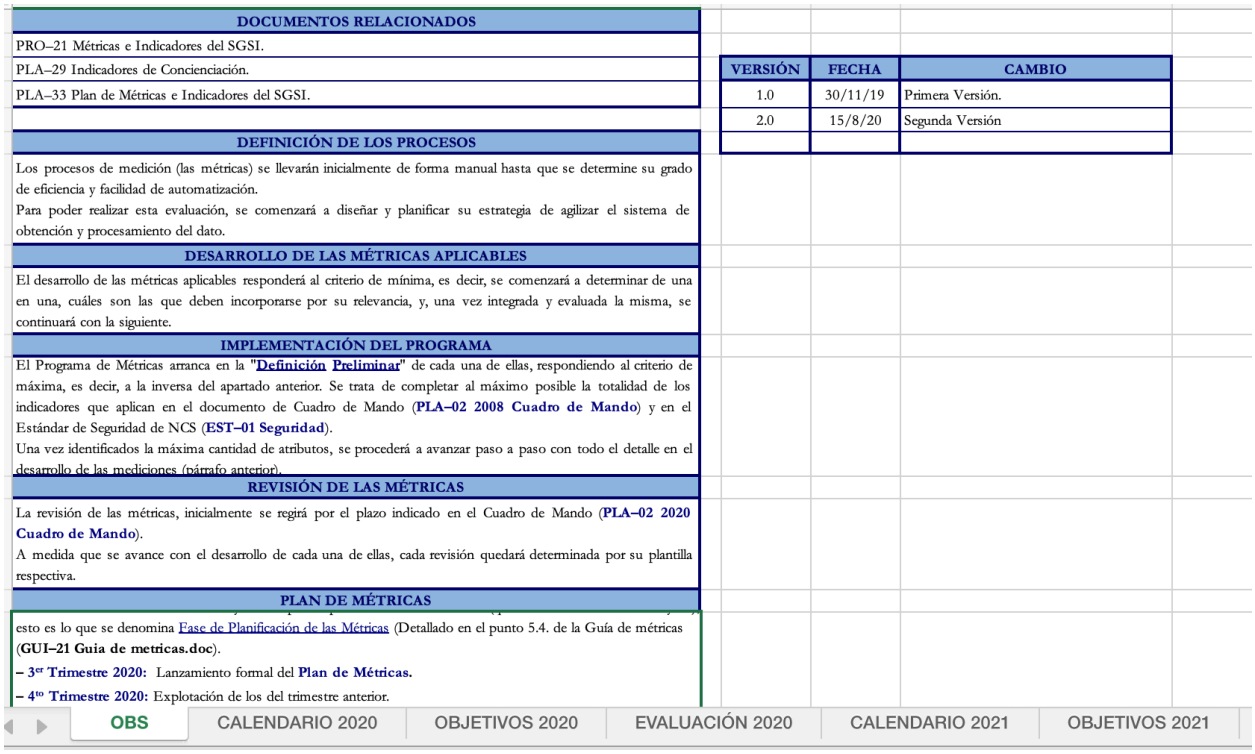
Los umbrales a alcanzar deben ser claramente medibles, por lo que pueden ser expresados en números, porcentajes, valores máximos o mínimos, etc. A continuación se presenta una tabla de ejemplo con los que se han definido para el caso práctico que venimos desarrollando:

Nº	Entidad	Atributo	Indicador	Umbral
(1)	RPO y RTO	Objetivos de recuperación	Estado de implantación de RPO y RTO en activos críticos.	100 %
			Pruebas y verificaciones de recuperación y comportamiento de RPO y RTO.	0,1 fallo en 10
(2)	KPIs	Indicadores imprescindibles de seguridad	Definición e implantación de KPIs	100 %
			Revisión, modificación e incorporación de nuevos KPIs	mínimo: 5 KPI/ año
(3)	IDS/IPS	Sistemas de tratamiento de intrusiones.	Configuración y actualizaciones	mínimo 1 actualiz./mes
			Evolución de falsos positivos y negativos	10 %/año
(4)	BBDD y Backups	Almacenamiento y resguardo de información	Indicadores de obsolescencia	Antelación 6 meses
(5)	Grandes equipos	Equipamiento cuyo coste supera los 15.000 €	Implantación de nuevos servidores	Demoras inferiores: 1mes
			Evaluación de rendimiento	Máximos 70%
(6)	Mejoras Anti DDoS	Protección perimetral	Grado de implantación	80 %
			Implantación y ajuste de umbrales	80 %
(7)	Formación	Capacitación del personal	Planificación e impartición de formación	Cubrir 90 %
			Medición de resultados	Nota prom: 7
8	DRP	Planes de recuperación.	Porcentaje de implantación	80 %
			Pruebas y mejoras	2 al año
(9)	SLAs	Acuerdos con proveedores.	Análisis de contratos y acciones concretas.	80 %
			Incorporación de nuevos SLAs	100 %

- Modelo de mediciones.

El modelo de mediciones puede realizarse de diferentes modos, en nuestro caso proponemos por medio de una plantilla de cálculo que respete al menos los siguientes aspectos (se presentan como imágenes de cada hoja que compone la plantilla).

Una primer hoja con los conceptos y definiciones básicas:



DOCUMENTOS RELACIONADOS
PRO–21 Métricas e Indicadores del SGSI.
PLA–29 Indicadores de Concienciación.
PLA–33 Plan de Métricas e Indicadores del SGSI.

VERSIÓN	FECHA	CAMBIO
1.0	30/11/19	Primera Versión.
2.0	15/8/20	Segunda Versión

DEFINICIÓN DE LOS PROCESOS

Los procesos de medición (las métricas) se llevarán inicialmente de forma manual hasta que se determine su grado de eficiencia y facilidad de automatización.
Para poder realizar esta evaluación, se comenzará a diseñar y planificar su estrategia de agilizar el sistema de obtención y procesamiento del dato.

DESARROLLO DE LAS MÉTRICAS APLICABLES

El desarrollo de las métricas aplicables responderá al criterio de mínima, es decir, se comenzará a determinar de una en una, cuáles son las que deben incorporarse por su relevancia, y, una vez integrada y evaluada la misma, se continuará con la siguiente.

IMPLEMENTACIÓN DEL PROGRAMA

El Programa de Métricas arranca en la "**Definición Preliminar**" de cada una de ellas, respondiendo al criterio de máxima, es decir, a la inversa del apartado anterior. Se trata de completar al máximo posible la totalidad de los indicadores que aplican en el documento de Cuadro de Mando (**PLA–02 2008 Cuadro de Mando**) y en el Estándar de Seguridad de NCS (**EST–01 Seguridad**).
Una vez identificados la máxima cantidad de atributos, se procederá a avanzar paso a paso con todo el detalle en el desarrollo de las mediciones (párrafo anterior).

REVISIÓN DE LAS MÉTRICAS

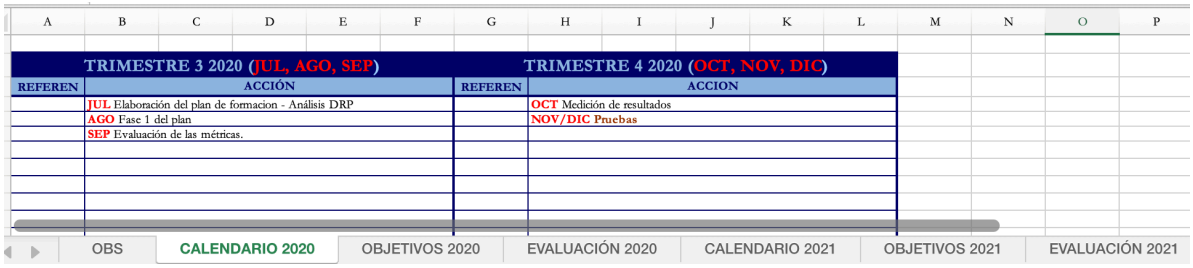
La revisión de las métricas, inicialmente se regirá por el plazo indicado en el Cuadro de Mando (**PLA–02 2020 Cuadro de Mando**).
A medida que se avance con el desarrollo de cada una de ellas, cada revisión quedará determinada por su plantilla respectiva.

PLAN DE MÉTRICAS

esto es lo que se denomina Fase de Planificación de las Métricas (Detallado en el punto 5.4. de la Guía de métricas (**GUI–21 Guia de metricas.doc**).
– **3er Trimestre 2020:** Lanzamiento formal del **Plan de Métricas.**
– **4to Trimestre 2020:** Explotación de los del trimestre anterior.

OBS | CALENDARIO 2020 | OBJETIVOS 2020 | EVALUACIÓN 2020 | CALENDARIO 2021 | OBJETIVOS 2021

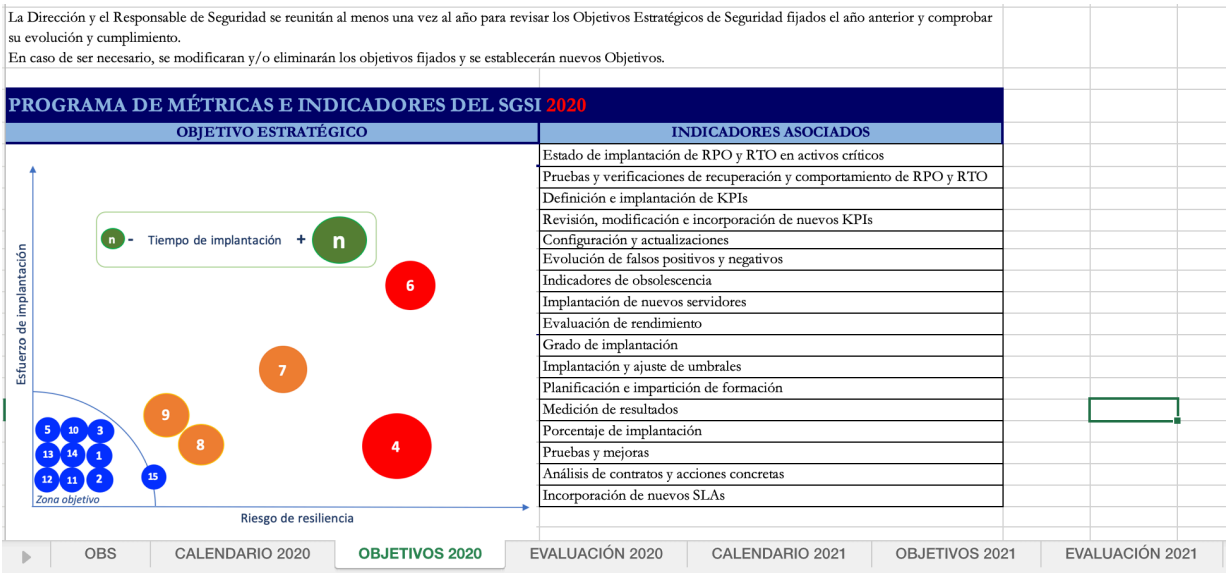
Una segunda en la que se puede desarrollar un calendario con las actividades, referencias acciones concretas a realizar, etc.:



TRIMESTRE 3 2020 (JUL, AGO, SEP)		TRIMESTRE 4 2020 (OCT, NOV, DIC)	
REFEREN	ACCIÓN	REFEREN	ACCION
	JUL Elaboración del plan de formacion - Análisis DRP		OCT Medición de resultados
	AGO Fase 1 del plan		NOV/DIC Pruebas
	SEP Evaluación de las métricas.		

OBS | CALENDARIO 2020 | OBJETIVOS 2020 | EVALUACIÓN 2020 | CALENDARIO 2021 | OBJETIVOS 2021 | EVALUACIÓN 2021

Una tercera que nos identifique claramente cuál es el objetivo estratégico que se desea cumplir, en nuestro caso para este primer año del ciclo de vida y cuáles son los indicadores buenos permitirán reconocer si se está desarrollando de acuerdo a lo definido. Como ya hemos venido avanzando de forma muy metodológica, en nuestro caso sería muy simple de cumplimentar, por ejemplo de la forma en que se presenta a continuación:



La Dirección y el Responsable de Seguridad se reunitán al menos una vez al año para revisar los Objetivos Estratégicos de Seguridad fijados el año anterior y comprobar su evolución y cumplimiento.
En caso de ser necesario, se modificaran y/o eliminarán los objetivos fijados y se establecerán nuevos Objetivos.

PROGRAMA DE MÉTRICAS E INDICADORES DEL SGSI 2020

OBJETIVO ESTRATÉGICO	INDICADORES ASOCIADOS
	Estado de implantación de RPO y RTO en activos críticos
	Pruebas y verificaciones de recuperación y comportamiento de RPO y RTO
	Definición e implantación de KPIs
	Revisión, modificación e incorporación de nuevos KPIs
	Configuración y actualizaciones
	Evolución de falsos positivos y negativos
	Indicadores de obsolescencia
	Implantación de nuevos servidores
	Evaluación de rendimiento
	Grado de implantación
	Implantación y ajuste de umbrales
	Planificación e impartición de formación
	Medición de resultados
	Porcentaje de implantación
	Pruebas y mejoras
	Análisis de contratos y acciones concretas
	Incorporación de nuevos SLAs

OBS | CALENDARIO 2020 | OBJETIVOS 2020 | EVALUACIÓN 2020 | CALENDARIO 2021 | OBJETIVOS 2021 | EVALUACIÓN 2021

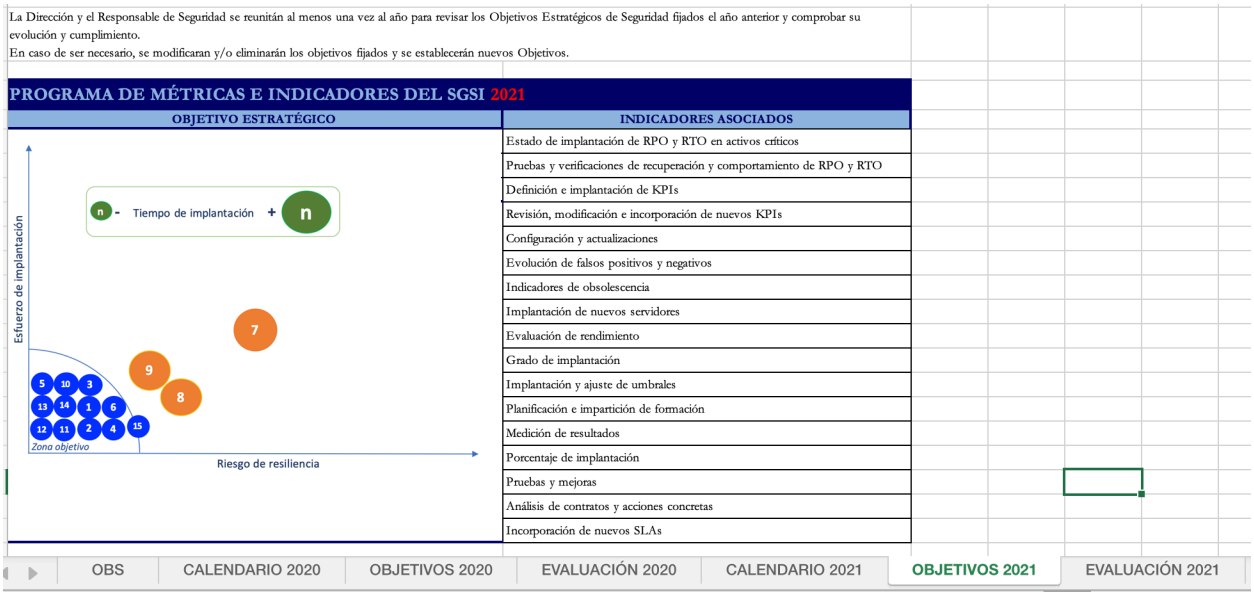
Como todo lo que estamos planificando debe ser posible de evaluar, pues de ello se trata la norma ISO 27004, deberíamos dejar preparado y hasta completado los hitos de control y resultados deseados, sobre la base de una hoja similar a la que presentamos aquí abajo:

Revisado por	Alejandro Corletti Estrada
Fecha	27/12/20

INDICADORES ELIMINADOS				INDICADORES MODIFICADOS				INDICADORES NUEVOS			
COD	REQUISITO	NOMBRE	MOTIVO	COD	REQUISITO	NOMBRE	MOTIVO	COD	REQUISITO	NOMBRE	MOTIVO

OBS | CALENDARIO 2020 | OBJETIVOS 2020 | EVALUACIÓN 2020 | CALENDARIO 2021 | OBJETIVOS 2021 | EVALUACIÓN 2021

Por último, siguiendo la misma lógica que aplicamos para el primer año en nuestro caso práctico, deberíamos desarrollar algo similar para el segundo:



La Dirección y el Responsable de Seguridad se reunirán al menos una vez al año para revisar los Objetivos Estratégicos de Seguridad fijados el año anterior y comprobar su evolución y cumplimiento.
En caso de ser necesario, se modificaran y/o eliminarán los objetivos fijados y se establecerán nuevos Objetivos.

PROGRAMA DE MÉTRICAS E INDICADORES DEL SGSI 2021

OBJETIVO ESTRATÉGICO	INDICADORES ASOCIADOS
	Estado de implantación de RPO y RTO en activos críticos
	Pruebas y verificaciones de recuperación y comportamiento de RPO y RTO
	Definición e implantación de KPIs
	Revisión, modificación e incorporación de nuevos KPIs
	Configuración y actualizaciones
	Evolución de falsos positivos y negativos
	Indicadores de obsolescencia
	Implantación de nuevos servidores
	Evaluación de rendimiento
	Grado de implantación
	Implantación y ajuste de umbrales
	Planificación e impartición de formación
	Medición de resultados
	Porcentaje de implantación
	Pruebas y mejoras
	Análisis de contratos y acciones concretas
	Incorporación de nuevos SLAs

OBS | CALENDARIO 2020 | OBJETIVOS 2020 | EVALUACIÓN 2020 | CALENDARIO 2021 | OBJETIVOS 2021 | EVALUACIÓN 2021

- Desarrollo de las mediciones aplicables.

Hemos ido desarrollando metodológicamente lo que nos propone el estándar ISO 27004 para poder tener un sistema de medición robusto que nos permita realizar un buen análisis de cómo evoluciona nuestra matriz de resiliencia.

Ahora nos queda darle forma a cada uno de esos indicadores que acabamos de definir y documentarlo correctamente. Esto nuevamente para ser prácticos, nos conviene trabajar por medio de una plantilla de cálculo, por supuesto que si contamos con alguna plataforma adicional que nos facilite esta tarea, pues mejor será.

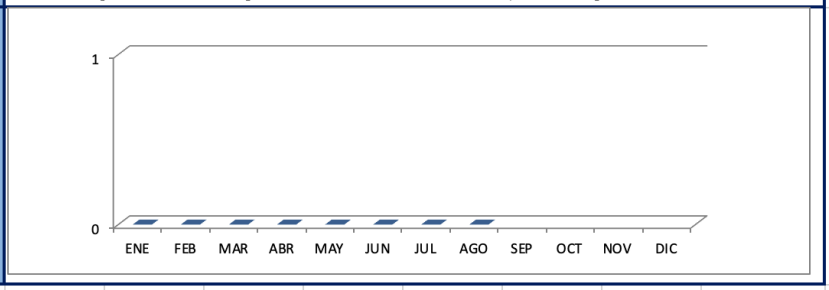
En esta plantilla, lo primero que debemos hacer es crear un índice con los indicadores a tener en cuenta. A continuación, presentamos un modelo, y como se puede apreciar, ya le asignamos un identificador a cada uno de los que hemos definido anteriormente:

CÓDIGO	NOMBRE	RESULTADO
I2020_01	Estado de implantación de RPO y RTO en activos críticos.	
I2020_02	Pruebas y verificaciones de recuperación y comportamiento de RPO y RTO.	
I2020_03	Definición e implantación de KPIs	
I2020_04	Revisión, modificación e incorporación de nuevos KPIs	
I2020_05	Configuración y actualizaciones	
I2020_06	Evolución de falsos positivos y negativos	
I2020_07	Indicadores de obsolescencia	
I2020_08	Implantación de nuevos servidores	
I2020_09	Evaluación de rendimiento	
I2020_10	Grado de implantación	
I2020_11	Implantación y ajuste de umbrales	
I2020_12	Planificación e impartición de formación	
I2020_13	Medición de resultados	
I2020_14	Porcentaje de implantación	
I2020_15	Pruebas y mejoras	
I2020_16	Análisis de contratos y acciones concretas	
I2020_17	Incorporación de nuevos SLAs	

Cada uno de estos indicadores, debemos ahora caracterizarlos con todo el detalle que nos ofrece este estándar. A continuación, a título de ejemplo, se presentan dos de ellos:

Estado de implantación de RPO y RTO en activos críticos.		
NOMBRE		Estado de implantación de RPO y RTO en activos críticos.
CÓDIGO		I2020_01
TIPO		Eficacia.
VALOR		Porcentaje (de implantación)
ESCALA		Porcentual.
PROPÓSITO		Evaluar el porcentaje de implantación de estos parámetros sobre activos críticos.
MÉTODO DE MEDIDA		Observación.
PROCEDIMIENTO		al finalizar el trimestre y siempre a final de año se hace la revisión.
CICLO DE VIDA	FRECUENCIA DE OBTENCIÓN	Anual.
	PERIORICIDAD DE ENTRADA	Variable
	FECHA DE OBTENCIÓN	Fecha
	FECHA DE VALIDEZ	Hasta la incorporación del siguiente activo crítico .
CRITERIOS VALIDEZ		Tasa de desvío < 10%
ALCANCE O DOMINIO		Activos críticos identificados por la matriz de resiliencia.
COMENTARIOS		El objetivo para el 2020 será un umbral al 100%
REPRESENTACIÓN		

INDICE | I2020_01 | I2020_02 | I2020_03 | I2020_04 | I2020_05 | I2020_06 | I2020_07 | I202

Configuración y actualizaciones (IDSs/IPSs)		
NOMBRE		Configuración y actualizaciones (IDSs/IPSs)
CÓDIGO		I2020_05
TIPO		Eficacia.
VALOR		Número.
ESCALA		Ordinal
PROPÓSITO		Comprobarel nivel de actualizaciones de estos dispositivos.
MÉTODO DE MEDIDA		Número de actualizaciones mensuales.
PROCEDIMIENTO		Se hacen comprobaciones en lapsos trimestralaes con revisión al final de año.
CICLO DE VIDA	FRECUENCIA DE OBTENCIÓN	Trimestrañ.
	PERIORICIDAD DE ENTRADA	Mensual.
	FECHA DE OBTENCIÓN	Cierre de mes.
	FECHA DE VALIDEZ	Anual.
CRITERIOS		Estos activos no son eficientes al estar desactualizados.
ALCANCE O DOMINIO		IDSs/IPSs
COMENTARIOS		Se verificará que la fuente de los repositorios de actualizaciones sea veraz y alcanzable por los activo en cuestión.
REPRESENTACIÓN		

INDICE | I2020_01 | I2020_02 | I2020_03 | I2020_04 | I2020_05 | I2020_06 | I2020_07 | I2020

- Implementación del programa.

  La implementación del programa, pasa por asignar los recursos necesarios, la asignación de tiempos suficiente y las responsabilidades de quién estará a cargo de estas evaluaciones para poder cumplir con el programa. En este punto se debe tener especialmente en cuenta el concepto de "segregación de funciones", que básicamente, significa que no se puede ser juez y parte. Es decir, es fundamental que persona o área que mida estos indicadores, no tenga relación con los propietarios o responsables de los mismos.

- Revisión de mediciones.

  La revisión de las mediciones es la tarea que nos informará si se está cumpliendo o no el plan. Esta actividad debería ser realizada por medio de un comité de seguridad que tenga un nivel jerárquico suficiente para adoptar decisiones y tomar medidas en caso de desvíos, pues justamente será quien decida sobre cómo encarar la fase "Act" aplicando las medidas correctoras, o acciones de mejora necesarias.

- Mejoras.

  En el caso que se detecte cualquier tipo de desvíos sobre los indicadores programados, los mismos se los considerará como hallazgos de la revisión y sobre los que hay que implementar un plan de acción.

  El plan de acción deberá ser propuesto por el responsable del activo crítico en cuestión, bajo el enfoque de ser abordable,. Es decir deberá solicitar y contar con los recursos necesarios para su implementación. Este plan de acción, es una buena práctica, que podamos integrarlo a alguna plataforma de ticketing para que quede registrado y genere las alarmas correspondientes sobre las nuevas fechas que se asignen al mismo.

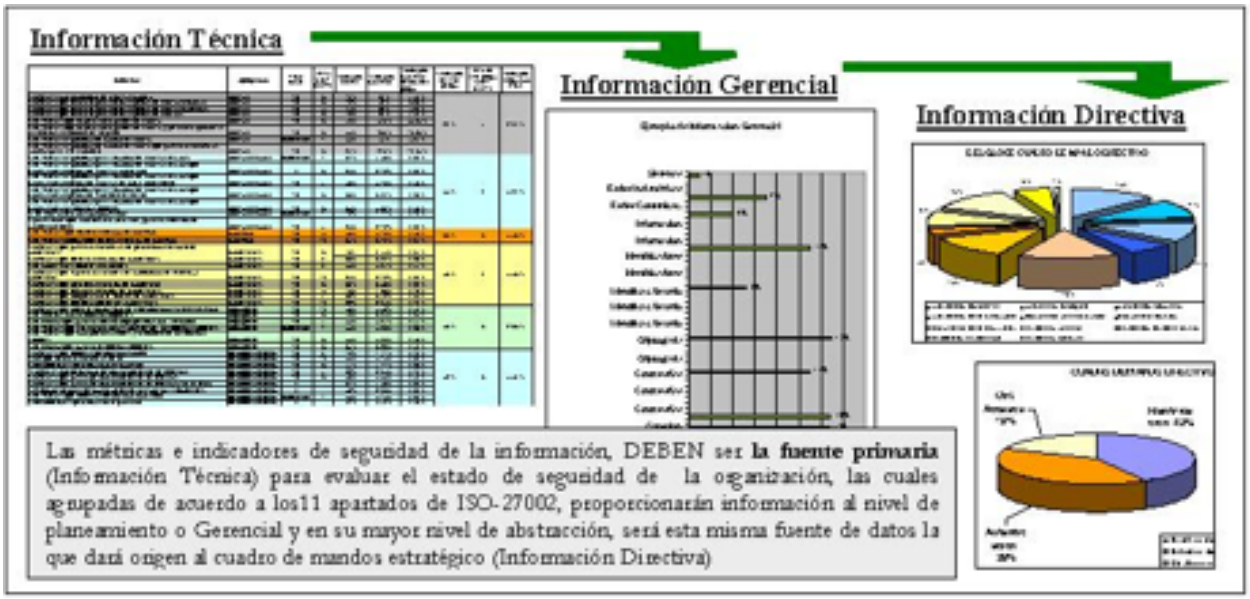
  Este plan de acción debería generar nuevos hitos de control sobre los indicadores del programa de medición, para que

puedan ser nuevamente analizados y evaluados, en la intención de verificar si el desvío se está encauzando, o no.

- Cuadro de mando.

El cuadro de mando, es la interfaz gráfica que consolida de forma visual nuestras métricas. Esta interfaz nos debe permitir de forma rápida, tener una visión clara de la evolución de nuestra matriz de resiliencia. La idea es contar con una visión, en cualquier momento, del ciclo de vida de nuestra infraestructura de ciberseguridad.

Es importante que nos presente la información que le interesa a cada nivel, pues un técnico necesitará mucho más nivel de detalle que la que le hace falta a un director, por lo que debería poder definirse roles o perfiles sobre este cuadro de mando para que cada uno pueda analizar la información que le interese. A continuación presentamos una imagen de ejemplo sobre estos diferentes puntos de vista.



KPI (key performance indicator) Indicadores Clave de Desempeño.

En la jerga empresarial, hoy en día es muy común encontrar definiciones que también debemos conocer y guardan relación, o hasta tal vez, podemos estar hablando de lo mismo. Una de ellas son los **KPI** (Key Performance Indicator). Se trata indicadores de rendimiento que utilizan las organizaciones para medir el desempeño en sus áreas y sobre los que debemos prestar especial atención. Cuando aparece la palabra "rendimiento", a mí en particular, siempre me viene a la cabeza que el rendimiento de cualquier cosa se puede medir sobre la base de dos ideas:

- Eficiencia.
- Eficacia.

Hace muchos años, una persona muy sabia me las explicó con la simpleza y sencillez que da la sabiduría y, jamás he vuelto a confundirlas:

> "*matar hormigas a martillazos es una forma tremendamente eficiente, pues cuando le aciertas a cualquiera de ellas la destrozas... pero claro, no es eficiente*".

Si me divierto matando hormigas en casa con un martillo, puede ser aceptable o discutible, pero a nivel industrial o empresarial, no suele ser el mejor método (aunque nadie me podrá decir que no es eficaz).

Un indicador de rendimiento debe ser eficiente y eficaz. Desde el punto de vista de resiliencia, son fundamentales pues cuando son eficientes y eficaces, nos permiten medir o evaluar el nivel alcanzado, mantener vivo el ciclo de vida de la seguridad, y la detección temprana de cualquier desvío que se produzca. Hasta ahora hemos desarrollado los aspectos de análisis de riesgo que nos permiten llegar a través de las métricas oportunas a definir indicadores de Ciberseguridad. Con estos indicadores, pudimos presentar una "Matriz de Resiliencia" que se ajuste al curso de acción que nuestra dirección seleccione. Este tipo de análisis se ha tratado de presentar de la forma más objetiva posible, considerando aspectos de ciberseguridad y resiliencia, pero veremos a continuación que podemos también priorizar algunos de estos indicadores sobre la base de conceptos que probablemente no tengan su origen en el análisis de riesgo, pero pueden sernos de suma utilidad para nuestra organización y desde el punto de vista de Ciberseguridad deben sincronizarse con el resto dela áreas.

Hay una regla mnemotécnica que me parece muy acertada a la hora de definir objetivos con éxito (en nuestro caso aplica perfectamente a KPIs) y

que se propone en el libro: "**Los criterios SMART El método para fijar objetivos con éxito**" de Guillaume Steffens. Esta regla nos presenta las siguientes características:

- **Specific** (eSpecíficos).
- **Measurable** (Medibles).
- **Achievable** (Alcanzables).
- **Relevant** (Relevantes).
- **Timely** (Temporales u oPortunos).

Desarrollemos con más detalle estos conceptos:

- Specific (eSpecíficos).

  El objetivo de un KPI debe ser entendible, claro y acotado. En estos términos siempre me ha gustado recurrir a mis orígenes militares y apelar a su experiencia milenaria. En este caso creo que la forma más concreta que veo es la forma en que se redacta la "Misión" de una orden de operaciones militar, la misma debe responder a lo que se denominan interrogantes básicos, y son: **Quién**, **que**, **cuándo**, **dónde** y **para qué**.

  Redactados de forma concreta serían:

  > *La compañía B del Regimiento de Infantería Aerotransportada 14 (Quién) atacará (qué), el día 25 de diciembre (cuándo) la cima del cerro "Resiliente" (dónde), con la finalidad de facilitar el avance de la brigada IV hacia el valle de los "KamPIngs" (para qué).*

  Acabamos de presentar algo totalmente específico.

- **Measurable** (Medibles).

  Ya hemos hecho hincapié sobre esta idea al desarrollar las métricas de la norma ISO-27004, pero creo importante remarcar nuevamente este concepto de "medible" pues he visto en

muchas ocasiones la definición de indicadores de rendimiento que eran totalmente subjetivos, o que su medición dependía de la hora, la persona, el software, el tráfico, etc., de forma que su medición no era representativa. Un objetivo medible es concreto: número, porcentaje, frecuencia, magnitud, fórmula, etc.

- **Achievable** (Alcanzables).

  Una de las cosas que más valoro de una certificación ISO-27001, es que no se exige que la organización, o el alcance esté securizado al 100%, el objetivo de una certificación de este tipo, es demostrar que se ha lanzado un SGSI de forma metodológica, con un análisis de riesgo serio, con umbrales bien definidos y con un plan de mejora responsable que a través del ciclo de vida que se está presentando, pueda demostrar que año a año se genera una mejora continua. La perfección es inalcanzable (y recordar que es enemiga de lo bueno), por lo que lo que nos debe identificar un buen KPI es un objetivo alcanzable, caso contrario, sin lugar a dudas será algo etéreo con resultado que jamás serán reales.

- **Relevant** (Relevantes).

  En todo el proceso que fuimos siguiendo en el libro, se ha intentado llegar, justamente a este concepto, a través de los recursos críticos, cuya explotación mal intencionada ocasione un alto impacto a nuestra empresa, así llegamos a presentar la matriz de resiliencia y la selección del curso de acción por parte de la dirección. Desde un enfoque metodológico, llegamos a poder identificar indicadores que son relevantes para nuestra organización y sobre los mismos desarrollamos todos sus campos parámetros, umbrales y calendario.

- **Timely** (Temporales u oporTunos).

  Para medir eficiencia, es sumamente importante la definición de hitos de control. Es decir, poner fechas concretas

con una periodicidad adecuada para que nos permitan analizar si vamos por el camino correcto o nos estamos desviando.

Según nuestro punto de vista, el concepto de KPI, hoy en día, está especialmente desarrollado y explotado en dos tipos da áreas: marketing y finanzas. En marketing se presta máximo interés en el impacto de llegada de campañas o cumplimiento de objetivos de difusión. En el área de finanzas, se centra la atención en los indicadores económicos de coste beneficio, inversiones, balance de resultados, etc.

Una página que nos pareció interesante para profundizar en este tema es: https://kpi.org

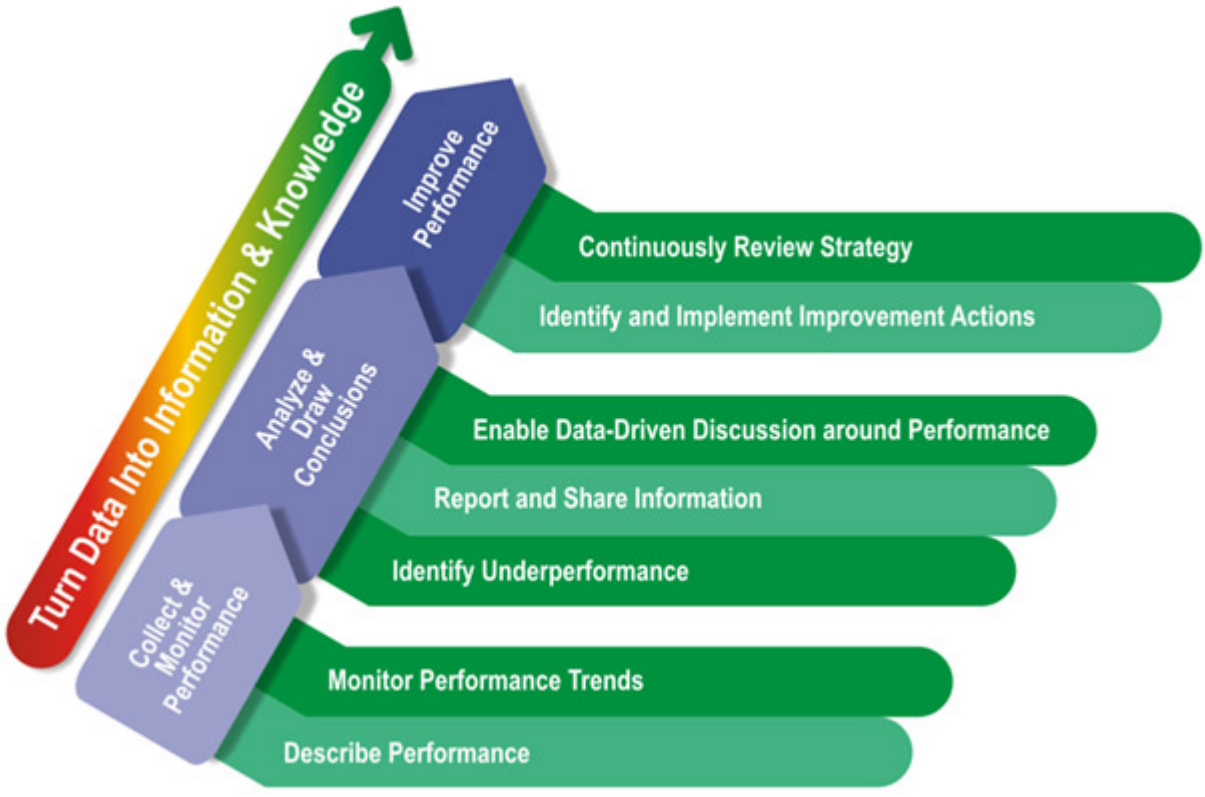


Imagen tomada de: https://kpi.org/KPI-Basics/Dashboarding-and-Analysiskpi-org

Hemos puesto este capítulo con el objetivo de presentar un enfoque que justamente nos permita relacionar el avance que tienen estos KPIs en las áreas mencionadas con temas de ciberseguridad y resiliencia, pues podemos considerar situaciones que seguramente nos permitirán ajustar más aún todos estos indicadores y métricas que hemos desarrollado hasta ahora.

Comencemos desarrollando algunos tipos de KPIs que suelen emplear las áreas mencionadas, para luego reflexionar y proponer asociaciones de los mismos en los temas que nos interesan en este libro.

- Importancia para la base del negocio.

  Cuando se aprueban los objetivos de la empresa para un período determinado (corto, medio o largo plazo), los mismos suelen estar relacionados al beneficio de la organización, por supuesto teniendo en cuenta todos los factores que permiten alcanzarlos en el marco legal del país o entorno en que se opere (medio ambientales, sociales, humanos, comerciales, electrónicos, financieros, regulaciones país, etc.). Los KPIs que se implementen en este concepto permitirán evaluar si el negocio vende, produce, genera, transporta, etc. lo planificado o se desvía de este tipo de objetivos.

- Indicadores financieros.

  Este tipo de indicadores, eminentemente monetarios, guardarán estricta relación con los balances de resultados, pérdidas o ganancias, intereses, préstamos, financiaciones, activos, amortizaciones, etc.

- Rebote y conversión.

  En marketing hay dos KPIs que suelen se prioritarios para evaluar resultados de campañas.

  - Tasa de rebote: Suele llamarse también abandono, y define el porcentaje de usuarios que han visitado un

servicio (página web, blog, publicidad, etc.), y que la han abandonado en un breve instante.

- Tasa de conversión: Se trata un poco de la inversa del anterior, y mide el éxito que ha tenido, o el porcentaje de usuarios que mantienen un cierto intervalo de tiempo en el servicio ofrecido.

En los párrafos anteriores, hemos puesto de manifiesto algunos casos de KPIs que seguramente emplearán otras áreas de nuestra organización. Independientemente que en ciberseguridad, nosotros los llamemos métricas o indicadores, o cualquier otra nomenclatura, lo mas probable es que esas áreas los llamen KPIs.

El aspecto al que queríamos llegar, es que nuestros indicadores en algún momento deberán sincronizarse, coordinarse, o al menos no ir en contraposición de los KPIs de estas áreas, pues de ser así estaríamos generando un conflicto en la organización, o una brecha de seguridad, pues posicionaríamos nuestros indicadores en una situación muy difícil de cumplir.

El problema está en que a cada uno de estos indicadores se ha arribado por caminos diferentes, pues el nuestro ha tenido su punto de partida en un "análisis de riesgo" de ciberseguridad, el de finanzas en una análisis económico y el de marketing, en las campañas que ha lanzado o lanzará.

Un ejemplo concreto y real, suele suceder cuando el área de marketing necesita lanzar una campaña en la que millones de clientes concurrirán hacia un determinado servicio que se prestará a través de la infraestructura de redes y TI de la organización. El área de marketing, justamente desea que su tasa de conversión sea máxima y la de rebote mínima, para que los futuros clientes dediquen tiempo a evaluar su campaña, y justamente no se desilusionen inmediatamente que "pinchan" en ese vínculo.

Desde el punto de vista de Ciberseguridad, seguramente opinemos bastante diferente, pues lo que quisiéramos, es poder minimizar la concurrencia, generar todos los Logs que sean necesarios, aplicar máximas reglas de filtrado, listas de control de acceso, procesos de validación y autenticación robustos, mecanismos de doble autenticación, empleo de criptografía robusta, calves de acceso con caracteres especiales y longitud aceptable, revisiones del proceso, etc. Todo esto sin lugar a dudas demorará el lanzamiento de la campaña, generará varios pasos intermedios,

certificaciones, validaciones, pruebas de maqueta, y por último demoras ante cada potencial cliente que "pinche" el enlace deseado.

Como puede apreciarse, tenemos un conflicto de intereses y los indicadores que estaríamos buscando cada área seguramente deberán conciliarse hasta llegar a un acuerdo entre las partes.

En resumen, hemos desarrollado este tema de los KPIs, pues es una realidad de toda empresa, es normal que sigan caminos diferentes en su definición e implantación, y o más importante de toda esta última parte, es que seguridad **no** puede ser un freno para los objetivos estratégicos de la empresa. Las medidas de Ciberseguridad siempre son molestas, pero debemos encontrar el equilibrio justo en la implementación de las mismas y sus acuerdos con todas las áreas de la empresa, sino sin lugar a dudas estaremos haciendo las cosas mal.

Nos ha sucedido muchas más veces de lo deseado, encontrarnos con áreas de seguridad que trabajan de forma excesivamente independiente del resto de la organización e imponiendo medidas que son trabas concretas al desempeño de otras áreas. El resultado de este tipo de conducción de áreas de Ciberseguridad es totalmente nefasto, pues tarde o temprano generan conflictos de interés y el resultado final, es que no se cumplen las medidas de seguridad, no se cumplen los hitos planificados, el ciclo de vida se desvirtúa, se termina dejando de lado la importancia de la seguridad, des jerarquizándola o reduciendo su capacidad de decisión y presupuestaria.

Es difícil encontrar este equilibrio justo (como en todo orden de esta vida…), pero nuestra recomendación sincera, es que hagáis todo el esfuerzo end conciliar vuestros "KPIs" con los de todas las áreas, por supuesto, cediendo hasta donde la seguridad lo permita sin dejar brechas, pero siempre dispuestos a escuchar y negociar hasta llegar a un consenso con todas las áreas.

13. Planes de formación y concienciación.

La norma **UNE-EN ISO/IEC 27002** de mayo de 2017, en su punto 7.2.2 "Concienciación, educación y capacitación en seguridad de la información", establece todos los conceptos que necesitamos tener en cuenta en este capítulo.

Como guía de implantación, nos propone que un "*programa de concienciación en seguridad de la información debería tener como objetivo el hacer a todos los empleados y, cuando corresponda, a los contratistas, tomar conciencia de sus responsabilidades en materia de seguridad de la información y los medios disponibles para ejercerla*".

Este programa debería estar alineado con las políticas y procedimientos de la empresa, como también con las medidas que se implanten. Debe diseñarse sobre la base de la función que desempeña cada empleado o área, sobre un calendario concreto y real, que permita que las actividades se repitan y den cobertura a nuevos empleados o cambios de función, actualizándose periódicamente para que incorpore las lecciones aprendidas sobre mejoras o incidentes en la empresa.

Esta es una de las actividades de control de una certificación sobre la norma **ISO 27001**, por lo que debe ser planificada y desarrollada de forma medible, con su propio ciclo de vida, y que permita la verificación de su grado de eficiencia dentro de la organización, por medio de indicadores como los que desarrollamos en el punto anterior.

Esta formación debería cubrir aspectos como:

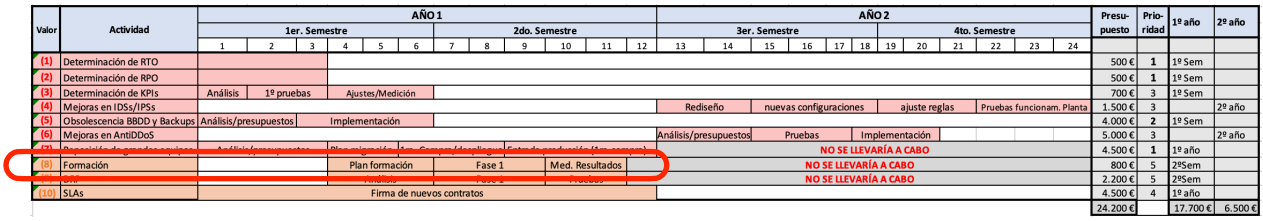
- Compromiso de la dirección.
- Conocimiento y cumplimiento de las normas y obligaciones de la organización.
- Responsabilidades y obligaciones del personal.
- Desarrollo de temas sobre los procesos básicos de seguridad.
- Acceso a los documentos y recursos de formación.

Este procedimiento, deberá tener una planificación periódica y es importante que los empleados entiendan el propósito de la ciberseguridad y el impacto que puede ocasionar sobre la empresa su propio comportamiento. Debería realizarse también un proceso de evaluación continua, que permita determinar el nivel de asimilación de los conocimientos transferidos.

Los pasos a seguir para el diseño de este plan deberían responder al menos a lo siguiente:

- Análisis de temática a cubrir.
- Diseño del plan.
  - Consolidación de temas.
  - Público al que irá dirigido.
  - Objetivos globales.
  - Recursos.
  - Distribución temporal.
- Gestión de la formación.
  - Objetivos puntuales.
  - Contenidos particulares.
  - Público al que va dirigido.
  - Metodología.
  - Duración.
  - Periodicidad y/o cronología.
  - Recursos específicos.
  - Perfil docente.
  - Sistema de evaluación.
  - Resultados finales.
  - Umbrales.
  - Medición de los resultados.

Para continuar analizando este procedimiento de forma práctica, pongamos de manifiesto, nuevamente, todo el trabajo sobre el que venimos avanzando, basado en la Estrategia de resiliencia que ha seleccionado la dirección de nuestra organización (curso de acción intermedio) y del cuál se ha manifestado que uno de los riesgos sobre los que se debería trabajar era justamente la Formación.



Valor	Actividad	AÑO 1												AÑO 2												Presupuesto	Prioridad	1º año	2º año
		1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				
(1)	Determinación de RTO																									500 €	1	1º Sem	
(2)	Determinación de RPO																									500 €	1	1º Sem	
(3)	Determinación de KPIs	Análisis		1º pruebas		Ajustes/Medición																				700 €	3	1º Sem	
(4)	Mejoras en IDSs/IPSs													Rediseño		nuevas configuraciones				ajuste reglas			Pruebas funcionam. Planta			1.500 €	3		2º año
(5)	Obsolescencia BBDD y Backups	Análisis/presupuestos			Implementación																					4.000 €	2	1º Sem	
(6)	Mejoras en AntiDDoS													Análisis/presupuestos		Pruebas			Implementación							5.000 €	3		2º año
														NO SE LLEVARÍA A CABO												4.500 €	1	1º año	
(8)	Formación				Plan formación			Fase 1			Med. Resultados			NO SE LLEVARÍA A CABO												800 €	5	2ºSem	
														NO SE LLEVARÍA A CABO												2.200 €	5	2ºSem	
(10)	SLAs	Firma de nuevos contratos																								4.500 €	4	1º año	
																										24.200 €		17.700 €	6.500 €

Sobre ese concepto de formación, cuando seguimos avanzando con el capítulo de "Ciclo de Vida", definimos sus "Indicadores".

(7)	Formación	Capacitación del personal	Planificación e impartición de formación
			Medición de resultados

Si revisamos con más detalle toda la secuencia de este análisis desde el principio, podríamos identificar focos concretos sobre los que deberíamos preparar acciones de formación, por ejemplo:

- Formación en incidentes y emergencias (ISO/IEC 27035-2:2016: tal cual indica en su cláusula 9. Crear conciencia y formación sobre incidentes de seguridad).
- Tal cual se expresa en el capítulo 12.12. Responsabilidades, obligaciones y funciones del personal.
- Protección de datos personales: Todo el personal de la empresa, deberá recibir formación al respecto y evaluar los resultados del conocimiento adquirido, desarrollando programas de formación que garanticen el claro conocimiento del tema por todo el personal contratado (interno y externo).
- Formación: Indicador (8) de la matriz de resiliencia.
- Ciberseguridad.

Sobre estas líneas, podemos ir dándole forma a este procedimiento, que lo presentamos otra vez bajo la forma de una plantilla de cálculo.

En primer lugar definamos cuáles serán los cursos que nos interesan, propongamos un método de impartición y pongámosle un código.

Nº	Código	Actividad	Métolo
1	C2020_01	Política de Seguridad	On Line
2	C2020_02	Responsabilidades, obligaciones y funciones del personal	On Line
3	C2020_03	Protección de datos personales	On Line
4	C2020_04	Curo básico de ciberseguridad	Semi presencial
5	C2020_05	Formación en incidentes y emergencias	Presencial
6	C2020_06	Ciberseguridad nivel medio	Presencial

Comencemos con el diseño de una planificación temporal para la impartición de los mismos.

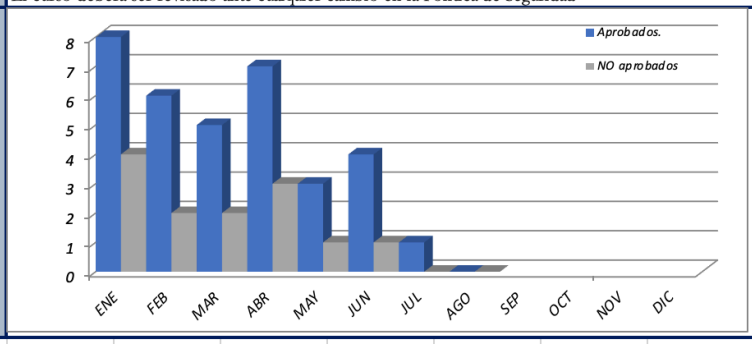
Nº	Código	Actividad	Métolo	AÑO 1												AÑO 2											
				1er. Semestre						2do. Semestre						3er. Semestre						4to. Semestre					
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	C2020_01	Política de Seguridad	On Line																								
2	C2020_02	Responsabilidades, obligaciones y funciones del personal	On Line																								
3	C2020_03	Protección de datos personales	On Line																								
4	C2020_04	Curo básico de ciberseguridad	Semi presencial																								
5	C2020_05	Formación en incidentes y emergencias	Presencial																								
6	C2020_06	Ciberseguridad nivel medio	Presencial																								

Luego podemos ya entrar en más detalle, intentando documentar con máxima precisión todos los conceptos que se fueron desarrollando en este capítulo.

Una muy buena práctica, es poder definir en este mismo documento, y con una lógica y estructura similar para cada curso todos los aspectos de los mismos, para lograr consolidarlos de forma visual, y que a su vez podamos explotar sus resultados para cualquier tipo de análisis o estadísticas. Otro aspecto que a nosotros nos ha sido de mucha utilidad, es poder integrara nuevos cursos de forma flexible y dinámica sobre el mismo procedimiento, por esta razón es que nos ha resultado muy práctico ejecutarlo por medio de una plantilla de cálculo.

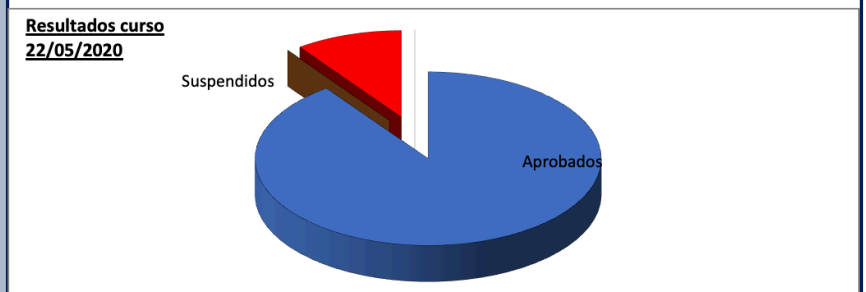
A continuación presentamos un par de hojas que nos muestran un modelo que solemos emplear para esta tarea.

En primer lugar podemos ver el curso número uno (**C2020_01**).

Política de Seguridad		
NOMBRE		Política de Seguridad
CÓDIGO		C2020_01
MÉTODO		On Line
OBJETIVO PUNTUAL DEL CURSO		Que el alumno tome conocimiento de la política de seguridad de la empresa, dejando constancia del mismo.
PÚBLICO AL QUE VA DIRIGIDO		Todo empleado que se incorpore a la empresa
CARÁCTER DEL CURSO		Obligatorio
DURACIÓN		4 horas
MÁXIMO DE ALUMNOS		Sin restricciones
SISTEMA DE EVALUACIÓN		Test On Line de selección múltiple
RESULTADOS FINALES		Calificación de 0 a 10
UMBRAL DE APROBACIÓN		5
MEDICIÓN DE RESULTADOS		Se analizarán incidencias ocurridas por desconocimiento de la Política de Seguridad y llevarán estadísiticas de las
PERFIL DOCENTE		El curso está diseñado "On Line" por el área de procedimientos de la empresa, centrando la atención en los puntos más importantes del procedimiento, por lo que el perfil docente, como curso en sí, no aplica aquí.
FECHAS PLANIFICADAS	INICIO	1/1/20
	FIN	31/12/21
	EVALUACIONES	Parciales en la finalización de cada alumno
	MEDICIÓN RESULTADOS	Semestrales
RECURSOS		Servidor moodle de la empresa, accesos a la intranet
COMENTARIOS		El curso deberá ser revisado ante cualquier cambio en la Política de Seguridad
CUADRO EVOLUCIÓN DEL CURSO		

Cursos | Calendario | C2020_01 | C2020_02 | C2020_03 | C2020_04 | C2020_05 | C2020_06

Para finalizar el capítulo y que puedan apreciarse los diferentes valores que aplican a una metodología On Line, de una presencial, presentamos a continuación el curso número cinco (**C2020_05**).

Formación en incidentes y emergencias		
NOMBRE		Formación en incidentes y emergencias
CÓDIGO		C2020_05
MÉTODO		Presencial
OBJETIVO PUNTUAL DEL CURSO		Que el alumno cuente con los conocimientos básicos para proceder adecuadamente ante incidentes o emergencias en redes y/o sistemas de TI.
PÚBLICO AL QUE VA DIRIGIDO		Todo empleado de la empresa
CARÁCTER DEL CURSO		Obligatorio
DURACIÓN		2 horas
MÁXIMO DE ALUMNOS		25 alumnos por sesión
SISTEMA DE EVALUACIÓN		Test al finalizar el curso
RESULTADOS FINALES		Calificación de 0 a 10
UMBRAL DE APROBACIÓN		6
MEDICIÓN DE RESULTADOS		Se analizarán a través de dos simulaciones o juegos de guerra Cibernética a realizarse durante el año (ver plantilla
PERFIL DOCENTE		El curso está impartido por el personal del área de seguridad de la empresa, sobre la base del temario diseñado específicamente para el curso sobre la base del prodecimiento de "Gestión de incidentes y emergencias de seguridad"
FECHAS PLANIFICADAS	INICIO	Fechas tentativas: 22/05/2020, 14/11/2020, 18/05/2021 y 15/11/2020
	FIN	mismas fechas (2 horas más tarde)
	EVALUACIONES	En la finalización de cada alumno
	MEDICIÓN RESULTADOS	Semestrales (en cada simulación) o ante la ocurrencia de cualqueir caso real.
RECURSOS		Aula de Informática, ordenadores, pizarra electrónica, proyector y acceso a Internet.
COMENTARIOS		El curso deberá ser revisado ante cualquier cambio en el prodecimiento de "Gestión de incidentes y emergencias de seguridad"
CUADRO EVOLUCIÓN DEL CURSO		

Cursos | Calendario | C2020_01 | C2020_02 | C2020_03 | C2020_04 | C2020_05 | C2020_06

14. Normas y estándares técnicos a tener en cuenta sobre resiliencia.

A lo largo del libro, fuimos presentando una serie de estándares, normas, regulaciones y guías que consideramos son necesarias para tener en cuenta en un sistema o red resiliente, a continuación reunimos en este capítulo todas las que se han mencionado en estas páginas.

Se presentan en el miso orden que fueron siendo mencionadas en el libro.

- **RFC-1244** "Site Security Handbook"

  https://www.rfc-editor.org/rfc/rfc1244.txt

  Si bien está obsoleta, la sigo considerando como una guía excelente a considerar en el desarrollo de una política de seguridad.

- la familia **IEEE-802.x** (Institute of Electrical and Electronics Engineers).

  el Subcomité 802 fue un proyecto creado en febrero de 1980, y de ahí viene lo de "80" (año) y "2" (febrero) y definen todo el conjunto de protocolos y medidas a implantar en redes LAN para el nivel de "enlace", considerando algunas veces también aspectos del nivel físico. Debemos tener en cuenta que el modelo TCP/IP por no ser un estándar oficial, algunos autores lo definen como un modelo de cinco niveles (físico, enlace, red, transporte y aplicación), sin embargo otros lo hacen como de cuatro niveles, pues agrupan el nivel físico y enlace en uno solo.

  Por lo tanto, en la familia IEEE 802.x (que es muy extensa), podemos encontrar todas las referencias que aplican a estos niveles inferiores de la pila TCP/IP, y la considero el primer punto de partida a la hora de investigar cualquier medida que aplique a los mismos.

- **Directiva 2008/114/CE**

DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008

sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

- **Ley 8/2011**

  La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

  https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

- **MAGERIT**

  Metodología de análisis de riesgo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) cuya autoría es del Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC) del Gobierno de España. Consta de tres libros "Método", "Catalogo de elementos" y "Guía de técnicas".

  https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- **ISO/IEC 27005** (tercera edición en Julio de 2018).

  "Tecnología de la información - Técnicas de seguridad - Información de gestión de riesgos de seguridad".

  https://www.aenor.com/normas-y-libros/buscador-de-normas/iso/?c=075281

- **ISO/IEC 31000** (segunda edición en febrero de 2018),

  Esta norma no se refiere únicamente a la gestión de riesgos de la seguridad de la información, sino que es genérica.

  En realidad, al igual que la serie ISO 27000, con la ISO 31000 se definió (o se intentó definir) también una familia de normas, pero la

realidad es que en la actualidad, dentro de esta serie, sólo están vigentes la que viene a continuación.

https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

- **ISO/IEC 31010** (segunda edición en junio de 2019)

  "Gestión de riesgos - evaluación del riesgo - evaluación técnicas del riesgo".

  https://www.iso.org/standard/72140.html

- **NIST SP 800-30.**

  Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Esta- dos Unidos.

  https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

- **NIST SP 800-39.**

  "Managing Risk from Information Systems - An Organizational Perspective".

  https://csrc.nist.gov/publications/detail/sp/800-39/final

- **OCTAVE**.

  "Operationally Critical Threat, Asset, and Vulnerability Evaluation" is a popular risk-based strategic assessment and planning technique from CERT;

  https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

- **INCIBE**

  Ofrece una guía muy sencilla que también podemos darle una mirada: ¡Fácil y sencillo! Análisis de riesgos en 6 pasos.

https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

- **ENISA (European Network and Information Security Agency)**

  Ofrece mucha información que deberíamos tener en cuenta, pero la que nos puede ser de mucha utilidad es esta guía de metodologías y herramientas: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools

  https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

- **Reglamento General de Protección de Datos de la Unión Europea (RGPD),**

  en el caso de España, la Agencia Española de Protección de Datos es la referente y posee toda la información al respecto.

  https://www.aepd.es/es

- **UNE-EN ISO/IEC 27001 de Mayo 2017.**

  Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

  https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058428

- **ISO/IEC 27004:2016.**

  Information technology -- Security techniques -- Information security management -- Measurement

  https://www.aenor.com/normas-y-libros/buscador-de-normas/iso/?c=064120

- **NIST 800–55 NIST** - Revisión 1 (julio 2008) (National Institute of Standards and Technology)

  "Performance Measurement Guide for Information Security" o "Guide for Developing Performance Metrics for Information Security"

  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

- **NIST 800–80**

  Publicado originalmente como borrador para comentario público el 5/4/2006, este documento nunca pasó a la publicación final. Se retiró el 1/11/2008 y fue reemplazado por el anterior: SP 800-55 Rev.1.

- **ISO/IEC 27037:2012**

  "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence". "Guía para la identificación, recolección, adquisición y preservación de evidencias"

  Este estándar fue revisado y confirmado por última vez en 2018, por lo tanto esta versión (2012) permanece actual

  https://www.iso.org/standard/44381.html

- **RFC 3227** "Guidelines for Evidence Collection and Archiving"

  Recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

  https://tools.ietf.org/html/rfc3227

  En INCIBE hay un buen artículo al respecto:

  https://www.incibe-cert.es/blog/rfc3227

- **UNE 71505** Gestión de evidencias electrónicas

Esta norma española, en realidad está compuesta por tres partes:

- **UNE 71505-1:2013**

  Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.

  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051411

- **UNE 71505-2:2013**

  Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.

  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0051412

- **UNE 71505-3:2013**

  Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.

  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0051413

UNE 71506:2013

Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.

https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051414

RD 03/2010 "Esquema Nacional de Seguridad" (ENS)

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

- **RD 04/2010 "Esquema Nacional de Interoperabilidad".**

  Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

  https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331

- **Centro Nacional de Inteligencia (CNI).**

  Dentro de la página Web del CCN podéis encontrar información de muy buena calidad:

  https://www.ccn.cni.es/index.php/es/

- **CCN-CERT**

  Una de las responsabilidades del CCN es el CERT (Computer Emergency Response Team), que en España, se lo conoce como "CCN-CERT".

  https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es

- **Guías de la familia 800**

  Todas ellas son una referencia de máximo nivel para organizar nuestros procedimientos de seguridad.

  https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

  Estas guías establecen unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. El listado completo de las mismas se encuentra en:

  https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

- **NIST 800-184**

"Special Publication 800-184 - Guide for Cybersecurity Event Recovery" de diciembre de 2016, que puede descargarse en:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

- **ISO/IEC 24762:2008**

  "Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services".

  https://www.iso.org/standard/41532.html

  Esta norma se publica en 2008 y, si bien ha sido anulada en 2014 (pues gran parte de ella, queda embebida en la norma ISO 27031 que se presenta a continuación)

- **ISO/IEC 27031:2011**

  Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.

  Esta norma es el reemplazo al **BS 25777**

  https://www.iso.org/standard/44374.html

- **UNE-EN ISO/IEC 27002:2017**

  Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).

  https://www.aenor.com/normas-y-libros/buscador-de-normas/une?c=N0058429

- **UNE-EN ISO 22301:2015**

  Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones.

La norma ISO 22301-2015 "Sistema de Gestión de Continuidad de Negocio", es la norma certificable sobre BCP. Al igual que la ISO 27001, también define los conceptos básicos para administrar y desarrollar el BCP.

Especifica la estructura y requerimientos para la implementación y mantenimiento de un "Business Continuity Management System (**BCMS**).

https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0054336

- **"Normas de la Autoridad Nacional para la protección de la Información Clasificada"**

  Recomendamos su lectura y se puede descargar en el siguiente enlace:

  https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf

- **BS EN 15713:2009** (British Standard)

  "Secure Destruction of Confidential Materials - a compete guide"

  https://www.bsia.co.uk/bsia-front/pdfs/204-id-en15713%20-%20a%20guide.pdf

- **UNE-EN 15713:2010**

  "Destrucción segura del material confidencial". Código de buenas prácticas. Es la versión española de la norma BS anterior, que se publicó en febrero de 2010.

  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0044792

- **Guía CCN-STIC 822**

  "Procedimiento de clasificación y tratamiento de la información clasificada - PR20"

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/539-ccn-stic-822-procedimientos-de-seguridad-anexo-ii/file.html

- **ISO/IEC 27035:2016**

  "Information technology — Security techniques — Information security incident management" (gestión de incidentes de seguridad de la información).

  Esta norma tiene dos partes:

  - **ISO/IEC 27035-1:2016**

    Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

    https://www.iso.org/standard/60803.html

  - **ISO/IEC 27035-2:2016**

    Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

    https://www.iso.org/standard/62071.html

- **UNE-EN 60839**

  "Sistemas electrónicos de control de accesos". Esta norma tiene dos partes:

  - **UNE-EN 60839-11-1:2014**

    Sistemas electrónicos de alarma y de seguridad. Parte 11-1: Sistemas electrónicos de control de acceso. Requisitos del sistema y de los componentes.

https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0052522

- **UNE-EN 60839-11-32:2017** (Ratificada)

  Sistemas electrónicos de alarma y de seguridad. Parte 11-32: Sistemas electrónicos de control de acceso. Monitorización del control de acceso basado en servicios Web. (Ratificada por la Asociación Española de Normalización en abril de 2017.)

  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0058109

Guías CIS (Center for Internet Security)

https://www.cisecurity.org/cis-benchmarks/

Guías del CCN-CERT de España.

https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

LSSI (Ley de Servicios de la Sociedad de la información) de España.

La Ley 34/2002, de 11 de julio, de "servicios de la sociedad de la información y de comercio electrónico"

https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Libros publicados por el mismo autor:

Todos ellos se encuentran disponibles para su descarga gratuita en formato electrónico en:

https://darfe.es/es/nuevas-descargas/category/5-lib

Si se desea su adquisición en formato impreso, estos sí son de pago (papel), también pueden ser adquiridos en:

https://darfe.es/es/comprar-libros

"**Seguridad por Niveles**" (2011)

"**Seguridad en Redes**" (2016)

"**Ciberseguridad, una estrategia Informático/Militar**" (2018)

"**Manual de la Resiliencia** (Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)"

15. Abreviaturas empleadas en el libro.

4R: Robustness, redundancy, resourcefulness, and rapidity

ACIDA:Autenticación (y si queréis también "Accesos"), Confidencialidad, Integridad, Disponibilidad, Accounting (o trazabilidad)

AENOR: Asociación Española de Normalización y Certificación

AEPD: Agencia Española de Protección de Datos

AET: Advanced Evasion Techniques

Anti DDoS: Anti Distributed Denial of Service

APT: Advanced Persistent Threat

BBDD: Bases de Datos

BCMS: Business Continuity Management System

BCP: Business Continuity Plan (ver también PCN)

BGP: Border Gateway Protocol

BS: British Standard

BSS: Bussines Support System
C4I2: Computación, comando, comunicaciones, control, inteligencia e informática

CAINE: Computer Aided INvestigate Environment

CCN: Centro Cripotológico Nacional de España

CEO: Chief Executive Officer

CERT: Computer Emergency Response Team

CIS: Center for Internet Security

CNI: Centro Nacional de Inteligencia de España

CNPIC: Centro Nacional para la Protección de las Infraestructuras Críticas

CPM: Critical Path Method

CSAE: Consejo Superior de Administración Electrónica

CSIRT: Computer Security Incident Response Team

DLP: Data Loss Prevention

DMZ: DeMilitarized Zone o Zona Desmilitarizada

DRP: Disaster Recovery Plan

EIGRP: Enhanced Interior Gateway Routing Protocol

ENISA: European Network and Information Security Agency

ENS: Esquema Nacional de Seguridad

EOC: Emergency Operations Center

FOA: First Office Application

FTP: File Transfer Protocol

FW: Firewall

HW: Hardware

HTTPS: Hiper Text transfer Protocol Secure

ICMP: Internet COntrol Messaging Protocol

ICT: Information and Communication Technology

ICTDR (ICT Disaster Recovery)

IDS: Intrusion detection System

IEEE: Institute of Electrical and Electronics Engineers

IEC: International Electrotechnical Commission

INCIBE: Instituto Nacional de Ciberseguridad (España)

IPv4: Internet Protocol Versión 4

IPv6: Internet Protocol Versión 6

IPS: Intrusion Prevention System

IRBC: I=ICT y RBC=Readiness for Business Continuity

IRC: Internet Relay Chat

ISO: International Standardization Organization

KPI: Key Performance Indicator o Indicadores Clave de Desempeño

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LGPL: GNU Lesser General Public License

LOPD: Ley Orgánica de Protección de Datos (España)

LSSI: Ley de Servicios de la Sociedad de la información (España)

MAC: Medium Access Control

MAGERIT:Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

MSTP: Multiple Spanning Tree Protocol

MZ: Militarized Zone o zona militarizada

NATO: North Atlantic Treaty Organization u OTAN: Organización del Tratado Atlántico Norte.

NIST: National Institute of Standards and Technology

NOC: Network Operation Center

NTP: Network Time Protocol

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

ONG:Organizaciones no gubernamentales

ONS: Oficina Nacional de Seguridad de España

OSPF: Open Short Path First (Protocol)

OSS: Operation Support System

OTP: One time Password

PCN: Plan de Continuidad de Negocio (ver también BCP)

PDCA: Plan-Do-Check-Act

PEPIC: programa europeo de protección de las infraestructuras críticas

PERT: Program Evaluation and Review Technique

PVST: Per VLAN Spanning Tree (Protocol)

RADIUS: Remote Authentication Dial-In User Service

RD: Real Decreto

RDP: Recovery Disaster Plan

RFC: Request For Comment

RGPD:Reglamento General de Protección de Datos de la Unión Europea RGPD

RMA: Reliability, Maintainability, y Availability o confiabilidad, mantenibilidad (o mantenimiento) y disponibilidad.

RPO: Restauration Point Objetive

RSTP: Rapid Spanning Tree Protocol

RTO: Recovery Time Objective

RTP: Real-time Transport Protocol

SCTP: Strem Control Transport Protocol

SDP: Session Description Protocol

SGSI: Sistema de Gestión de la Seguridad de la Información

SIEM: Security Information and Event Management

SIP: Session Initiation Protocol

SLA: Service Level Agreement o Acuerdo de Nivel de Servicio

SMART: Specific (eSpecíficos), Measurable (Medibles), Achievable (Alcanzables), Relevant (Relevantes) y Timely (Temporales)

SNMP: Single Network Monitor Protocol

SOC: Security Operation Center

SP: Special Publication o Standard Procedure

SPB: Shortest Path Bridging (Protocol)

SSO: Single Sign On

STP: Spanning Tree Protocol (Protocol)

SW: Software

TACACS: Terminal Access Controller Access Control System

TCP/IP: Transport Control (o Connection) Protocolo / Internet Protocol

TI: Tecnologías de Información

TIA/EIA: Telecommunications Industry Association / Electronic Industries Alliance

TIC: Tecnologías de Información y Comunicaciones

UDP: User Datagram Protocol

UNE: Una Norma Española

UTP: Unshield Twisted Pair (Cable)

VSAT: Very Small Aperture Terminal

WiFi: Wireless Fidelity

WWW: World Wide Web

"Manual de la Resiliencia *(Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)",* se trata de la cuarta obra técnica de **Alejandro Corletti Estrada** que desarrolla temas de Redes y Seguridad.

Esta nuevo libro es la continuación de los anteriores: "**Seguridad por Niveles**" (*2011*), "**Seguridad en Redes**" (*2016*) y "**Ciberseguridad, una estrategia Informático/Militar**" (2018). Todos ellos son el resultado de muchos años de apuntes, clases, cursos, artículos, conferencias y auditorías de seguridad que han sido recopilados y presentados de forma técnica, con muchos ejemplos, procedimientos, plantillas y ejercicios.

En esta ocasión desarrolla más específicamente el problema de "Ciberresiliencia", aspecto que necesita tener hoy en día cualquier red o infraestructura de TI ante la realidad de sufrir incidentes de ciberseguridad, o también fallos o desperfectos técnicos que siempre están omnipresentes.

La "Información" es el centro del libro, ***"Lo crítico es la INFORMACIÓN... no las infraestructuras"***. Como bien más preciado de toda empresa, esta páginas nos presentan métodos, acciones y procedimientos concretos para custodiarla, protegerla y mantenerla íntegra durante todo su ciclo de vida.

Tenemos el honor de contar, en el capítulo 3 "*El poder de la Información y las realidades inexistentes*", con la invalorable aportación del General de División **Evergisto de Vergara** que, con su claridad de pensamiento y visión actual del arte de la guerra, nos presenta este nuevo dominio militar de "la opinión".

El libro, una vez más, como los anteriores, está disponible en su versión digital bajo licencia **"Copyleft"** para su libre descarga y difusión sin fines de lucro en la página Web: **www.darFe.es**. Se recomienda especialmente para su uso en todo tipo de ámbito de docencia por su marcado enfoque metodológico.

Alejandro Corletti Estrada:

Es Doctor en Ingeniería Informática, MBA. Fue militar, Jefe de Redes del Ejército Argentino, profesor universitario de las materias Redes y Comunicaciones y Director del Centro de Investigación en Seguridad Informática de Argentina (CISI.ar), y actualmente docente del master en Ciberseguridad de la Universidad Alfonso X y Director de la empresa "**DarFe Learning & Consulting S.L.**". Vino a Madrid en el año 2000, lugar donde actualmente vive. Se ha desempeñado como consultor experto y asesor en temas de seguridad informática y Redes en muchas empresas. Ha disertado en varios congresos internacionales, seminarios y publicado artículos siempre relacionados a seguridad y redes de ordenadores.

Fundación UAX

www.darFE.es

UAX UNIVERSIDAD ALFONSO X EL SABIO