Gestión de la ciberseguridad

PID_00262371

Léonard Janer García

Tiempo mínimo de dedicación recomendado: 16 horas

Universitat Oberta de Catalunya

Léonard Janer García

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Jordi Ayza Graells (2019)

Primera edició: febrer 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Disseny: Manel Andreu
Realització editorial: Oberta UOC Publishing, SL

Índice

1. Gestión de la ciberseguridad

1.1. Estrategia de la ciberseguridad industrial. Amenazas, análisis y gestión de riesgos

1.1.1. Estrategia de ciberseguridad

En los últimos años, han ido en aumento los conceptos asociados a la seguridad digital. Nos hemos familiarizado con los términos ciberseguridad, seguridad de la información o seguridad IT, entre otros. Todos estos conceptos tienen una fuerte relación entre ellos, pero sin duda lo primero que debemos hacer es tenerlos claros, y cuál es su relación con nuestros activos y con los riesgos que nos rodean.

Hemos de ser capaces de diferenciar claramente los conceptos de *privacidad*[1] con los de *seguridad*.

(1)El blog de Bruce Schneier siempre es un buen referente en ciberseguridad (189)

En un sistema de computación, la seguridad (seguridad de los sistemas de computación, seguridad de los ordenadores, seguridad de las computadoras) está íntimamente relacionada con los procesos y el conjunto de medidas y controles que procuran asegurar la confidencialidad, la integridad y la disponibilidad[2] de los activos del propio sistema. Cada uno de los tres conceptos tiene su particular importancia:

(2)CIA, acrónimo del inglés *confidentiality, integrity and availability*.

1) Confidencialidad, para garantizar solo los accesos autorizados a los activos, y la protección contra la divulgación/revelación de información[3].

(3)En inglés se utiliza el término *disclosure*.

2) Integridad, para garantizar que no se modifica de forma intencionada una información. La modificación puede ser parcial (como podría ser modificar una parte de un contrato, de unos datos capturados por unos sensores, o de unos registros de entrada en una zona de acceso restringido), o total (incluyendo la total destrucción de la información).

3) Disponibilidad, para garantizar por un lado el acceso a la información, y por otro, su uso, en la forma requerida, en el tiempo oportuno o necesario y de forma segura, garantizada. Si pensáramos en suministros básicos (como agua, electricidad, gas…), estaríamos diciendo que se garantiza que, cuando se va a abrir el grifo, va a salir agua, pero además que el agua es agua, y que ha pasado todos los controles de salud perceptivos. Si pensamos en un sistema de computación, que cuando por ejemplo necesitamos acceder a una información que previamente se haya guardado en disco, cuando vayamos a requerir

el acceso, vamos a poder (tener los permisos, el sistema de disco estará disponible…) acceder a la información del disco, y además, que la información que vamos a recuperar será la que previamente habremos almacenado.

En estos sistemas de computación, los activos que vamos a procurar proteger serán de tres tipos:

1) Dispositivos físicos del sistema[4], tales como podrían ser los sistemas completos (servidores, teléfonos móviles, tabletas, ordenadores de sobremesa, ordenadores portátiles…), o los propios componentes internos de los mismos (memoria, discos, pantallas, teclados, puertos de conexión con el exterior USB, Ethernet o de cualquier otro tipo, fuentes de alimentación…) que son la base para el propio sistema completo.

(4)En inglés se utiliza el término *hardware devices*.

2) Dispositivos de red (de interconexión), en un primer nivel, los propios sistemas de cableado, pero sobre todo los dispositivos activos de interconexión como los conmutadores, o los encaminadores[5] que deben garantizar el acceso remoto a los dispositivos físicos. De nada nos sirve proteger los servidores, si no tenemos el mismo nivel de control y garantía sobre los dispositivos que intercomunican los servidores con los clientes en los que están trabajando los usuarios.

(5)En inglés se utiliza el término *switches, routers*.

3) Los elementos de la capa llamémosla lógica, en la que tenemos los sistemas operativos que se están ejecutando en todos y cada uno de los dispositivos, como los elementos de más bajo nivel, como podrían ser los *drivers* o el *firmware* de algunos elementos, o cualquier programa (software) que se esté ejecutando en el sistema de computación.

Como vemos, cuando hablamos de seguridad, el campo de trabajo se nos ha ensanchado de forma muy rápida.

Qué pasa si ahora tratamos de hacer foco en el concepto de seguridad de la información. Lo primero que debemos entender es que no se utiliza el término seguridad de los datos, sino de la información[6]. Por lo tanto, veamos qué son datos, y qué es información:

(6)*Big data*, el mundo de las promesas, donde parece que todo será posible…, y donde a través del análisis, traspasaremos las fronteras de los entornos de comercio electrónico, y portales web, para abarcar todos y cada uno de los sectores verticales de nuestra economía –el sector financiero, la fabricación, los transportes, el sector de suministros y energía, el sector de salud, alimentación y bio…–, que estarán todos íntimamente ligados con la capacidad de interconectar grandes cantidades de sensores (y actuadores) que van a ser la base de la industria 4.0.

1) Los **datos** en su definición más completa (y a la vez simple) son la representación digital de cualquier cosa en cualquiera de sus posibles formas (todo aquello que pueda representarse en forma digital[7]).

2) La **información** se extrae de los datos, y no es más que datos interpretados en un contexto determinado (un mismo dato puede representar informaciones diferentes en función de su contexto).

Es importante entender que los datos que disponemos para convertirlos en información pueden encontrarse en forma estructurada o en forma desestructurada:

(7)Una muy buena fuente de definiciones que siempre ha de tenerse a mano es el diccionario de la SNIA (Storage Networking Industry Association) (190) o los extensos recopilatorios de la NIST (National Institute of Standards and Technology) (191).

1) Datos estructurados: representa aquellos datos que suelen almacenarse en forma de bases de datos (con sus registros y sus campos) u hojas de cálculo, que mantienen una forma regular de almacenamiento y ordenación (registros, campos, filas…).

2) Datos no estructurados: podemos considerar que son aquellos datos que no están almacenados en forma de base de datos o tablas lógicas en formato 2D (como podría ser una tabla o una hoja de cálculo). Representan la mayoría de datos que podemos encontrar en internet y en los sistemas de información de las empresas y los individuos. Tenemos muchos datos, pero la información no siempre es fácil de extraer de los datos, precisamente por la falta de estructuración y organización.

Algunos autores también hacen referencia a datos semiestructurados, que serían aquellas fuentes de datos, como podrían ser ficheros de lenguajes de marcas (HTML, XML), que tienen una cierta organización de la información. Incluso podríamos aquí incluir los ficheros de Office que tienen una cierta estructuración con las propiedades del documento o sus macros.

Estrechamente vinculado con los datos (y la información que de ellos podemos extraer), es importante tener conciencia de dónde y cómo se van a almacenar todos estos datos. Aquí vamos a introducir brevemente los conceptos asociados a la provisión de servicios en el entorno del almacenamiento y los sistemas (1) que aportan flexibilidad a las soluciones empresariales de gestión de las infraestructuras de sistemas, con dos arquitecturas típicas (que comparamos en lo que hace referencia al coste y a la escalabilidad en la figura 1):

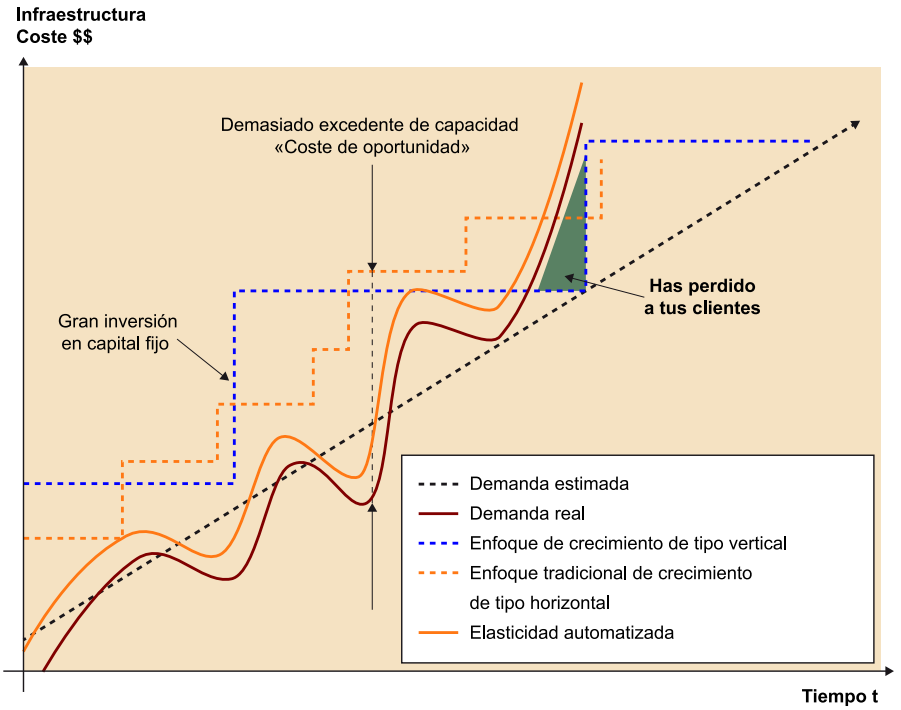
(8)En inglés se utiliza la terminología *scale-up*.

1) Las soluciones de escalado vertical[8]: en las que se lleva a cabo una fuerte inversión en los recursos de red y sistemas disponibles, de tal forma que en el momento que se están colapsando los sistemas se mejoran sus prestaciones (pasamos de un sistema que tenía un disco de 200GB a otro con 2TB y así sucesivamente).

(9)En inglés se utiliza la terminología *scale-out*.

2) Las soluciones de escalado horizontal[9]: en las que para aumentar los recursos disponibles no se mejoran las prestaciones de una unidad, sino que se replican más unidades de servicio. Si el disco se nos quedó pequeño, no cambiamos el disco (de 200GB a 2TB), sino que incorporamos nuevas unidades de disco (por ejemplo, podríamos pasar a tener 4 unidades de 500GB que juntas nos sumarían los 2TB, y que en caso de necesitar un incremento a 3TB, podríamos solucionar con dos nuevas unidades de los mismos 500GB, en lugar de cambiar la unidad de disco).

Figura 1. Coste y escalabilidad de las soluciones verticales y horizontales



La provisión de soluciones en Cloud para los servicios de sistemas IT se puede dividir en las siguientes formas de provisión:

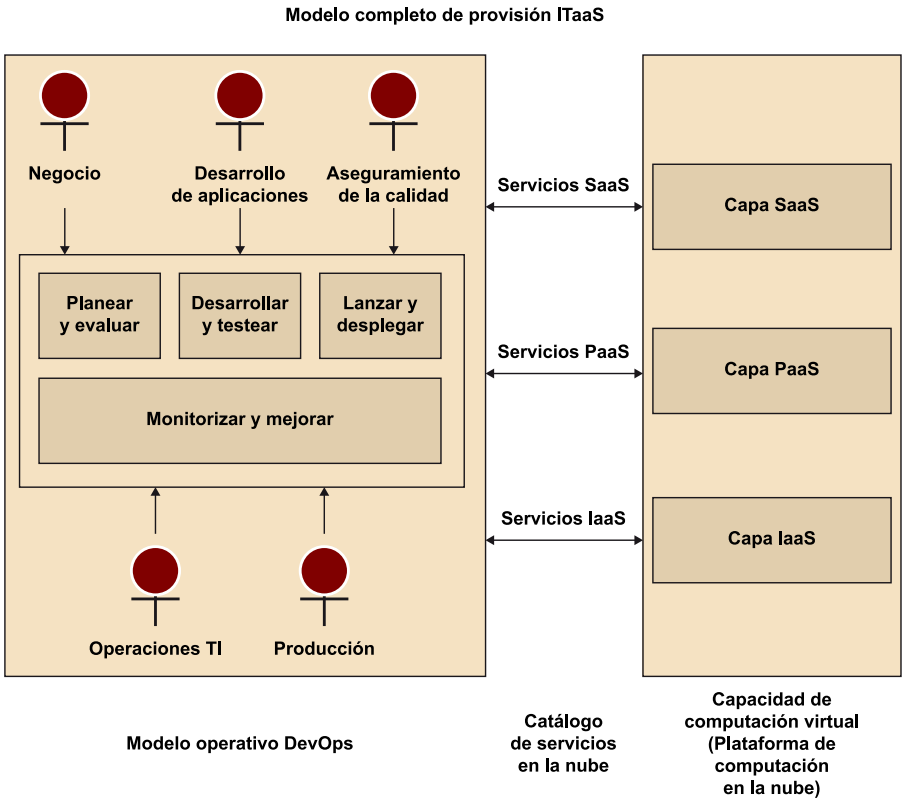
1) IaaS (infraestructura como servicio): en este caso, el servicio que se entrega a los clientes es la propia infraestructura física de los sistemas. Nos permite obviar la problemática de la adquisición y gestión de los equipos. Cada uno de los recursos (propios de un centro de procesos de datos) se ofrece en forma de servicio que podrá ser contratado por uso (bajo demanda). Solo se ofrece el equipo, no el software, ni las aplicaciones que se ejecutarán en él. Nos permite escalar de forma muy rápida si las necesidades de hardware aumentan.

2) PaaS (plataforma como servicio): en este caso, el servicio nos permite disponer de un completo entorno de desarrollo en Cloud, con todos los recursos necesarios. Nos permite disponer de las herramientas para desarrollar que es nuestro negocio, sin preocuparnos de las mismas. Si necesitamos una determinada herramienta para un momento puntual del desarrollo, la vamos a poder desplegar de forma inmediata y utilizarla sin la complicada gestión que tendríamos que hacer si tuviéramos, por ejemplo, que adquirir una licencia de la misma para su uso, o la instalación y configuración de la misma para, una vez dispongamos de licencia, poder utilizarla en nuestra operación, quizás por muy poco tiempo. Nos permite centrarnos en el desarrollo sin pensar en la provisión de las herramientas; estas las obtendremos a través de nuestro proveedor de servicios. Obviamente, si trabajamos con un modelo de plataforma como servicio, también estaremos (en primer lugar) utilizando el modelo de infraestructura como servicio (pues primero necesitaremos el servidor, y luego la plataforma de desarrollo), si bien la solución PaaS incorpora la solución IaaS.

3) SaaS (software como servicio): en este caso, los servicios que contratamos no son solo de infraestructura, ni de soluciones de desarrollo, o de sistema operativo, sino básicamente (siempre por encima de las anteriores obviamente) las soluciones de aplicaciones comerciales para el funcionamiento de nuestra actividad operativa (podríamos, por ejemplo, pensar en la solución de correo electrónico corporativo, las herramientas de ofimática…).

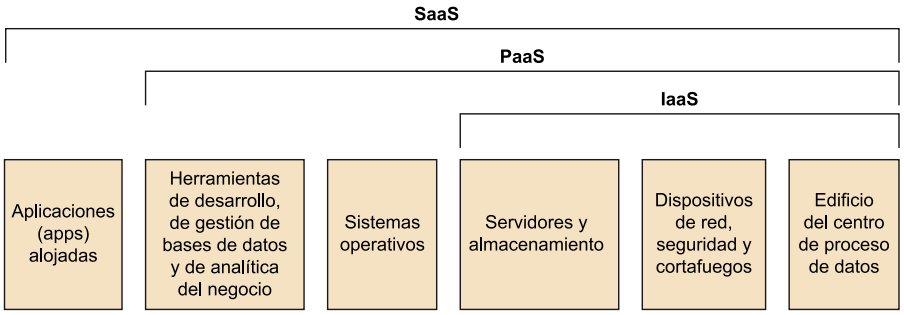
4) ITaaS (IT como servicio) (2): Este podría ser el último eslabón de la provisión de servicios en Cloud. No contratamos la infraestructura, ni el sistema operativo, ni las aplicaciones (corporativas), sino toda nuestra estructura IT, en forma de una plataforma integrada de personas, procesos, prácticas, estructuras de gobierno y herramientas que nos permitan alinear nuestro negocio, nuestra organización con nuestras necesidades IT.

Figura 2. Modelo de provisión de servicios ITaaS



En la figura 3, podemos ver una representación gráfica con los servicios que ofrece cada una de estas soluciones (3). Además, en la figura 2 vemos la relación entre todos los modelos, integrados en el modelo completo de ITaaS.

Figura 3. Diferentes soluciones de provisión de servicios en Cloud



Volviendo al punto que nos interesa, de la seguridad de la *información*[10], recordemos, pues, que la información no es más que un activo (dato en un contexto) que es de importancia para quien ha interpretado la información, y que puede estar almacenado en muy diversas formas: digitalmente (quizás siempre acabe en esta forma, para su posterior manipulación), impresa (cuantos documentos no tendremos almacenados en nuestros archivos), manuscritos, en forma de lenguaje hablado, gestos... En función de si hablamos de datos o de información, podemos en cierta forma intercambiar los conceptos de seguridad de la información o seguridad de los datos.

(10)En algunos entornos (sobre todo en inglés) se suele utilizar la abreviación InfoSec, para referirse al término de *information security*.

De acuerdo con la ISO 27000, de la que hablaremos extensamente en el capítulo 2, se define el término *InfoSec* como los procedimientos y controles necesarios y aplicados para preservar la confidencialidad, la integridad y la disponibilidad (CIA) de la información. Además, debe garantizar y preservar también la autenticidad y la confiabilidad de la información. Es a través y gracias a la seguridad de la información, con sus mecanismos de no repudio y de trazabilidad[11], que podemos hacer un seguimiento de todos los procesos en una organización. Solo puede haber trazabilidad si garantizamos la seguridad de la información. A través de garantizar el no repudio y la traza.

(11)En inglés se suele utilizar el término *accountability*.

El tercero de los términos que nos interesa es el de la seguridad IT. Las infraestructuras IT (*information technology*, tecnologías de la información, y en algunos casos las comunicaciones) representan, en la actualidad, una infraestructura crítica en prácticamente cualquier organización. Por lo tanto, la seguridad IT buscará establecer y garantizar una infraestructura IT sostenible, segura, que siga y cumpla las normas y regulaciones pertinentes y vigentes, robusta y confiable para garantizar de forma consistente un adecuado y conveniente soporte tecnológico a todos los usuarios, tanto si son empleados, como clientes o proveedores, o usuarios externos. Cuando el enfoque se desplaza, pues, hacia la seguridad IT, el aspecto más importante es el de la operatividad (debemos garantizar la continuidad del negocio, soportado sobre una infraestructura IT cada vez más crítica). Los activos a proteger están todos relacionados con la infraestructura y, por lo tanto, abarcarán todos los aspectos propios de la seguridad de los sistemas de computación, como los de la seguridad de la información, y cada vez tendrán más importancia los aspectos relacionados con las comunicaciones, pero siempre desde la perspectiva de la operatividad.

Si de alguna forma queremos comparar los aspectos fundamentales de la seguridad IT con los de la seguridad de la información, debemos entender que la primera tiene un importante enfoque tecnológico y que, por lo tanto, hará referencia a todos aquellos aspectos relacionados con el entorno y la infraestructura IT: los cortafuegos (*firewalls*), los sistemas antivirus, los escaneadores de vulnerabilidades, los test de penetración (*pentesting*), los sistemas de detección y prevención de intrusiones (IDS –*intrusion detection system*– e IPS –*intrusion prevention system*), las tecnologías de computación forense, los sistemas de control de acceso, la seguridad en redes, los sistemas de monitorización, la gestión de cambios y actualizaciones (*patch management*), y, obviamente, todo lo relacionado con la encriptación y cifrado de los datos.

Por otro lado, la seguridad de la información está más orientada al negocio, y su primer foco está más hacia la propiedad: propiedad intelectual, cumplimientos normativos, integridad de negocio (integridad financiera), espionaje industrial, privacidad de los datos, gobernanza, gestión de crisis, continuidad de negocio, análisis de riesgos…

Es muy importante que siempre se tenga el foco en que la seguridad IT es tecnología y operaciones, y que la seguridad de la información es negocio y estrategia. En muchas organizaciones, de hecho, los responsables de ambos ámbitos suelen ser dos figuras diferentes, con perfiles y responsabilidades diferentes (y en algunos aspectos incluso ciertamente contradictorias).

Acabemos, pues, nuestro periplo por las definiciones de base con el concepto de ciberseguridad. Nos encontramos ante un concepto relativamente joven (pongamos que emerge a partir de la última década del siglo pasado) y, por lo tanto, aún no existe una plena convergencia en su definición (como sí sucede en los términos anteriores):

1) Una definición simple nos sitúa en un subconjunto de la seguridad de la información, en tanto hace referencia a la información en lo que podríamos denominar el ciberespacio[12]. En general, el prefijo *ciber* nos indica términos asociados o relacionados con internet… En esta definición, que en un punto de partida puede parecer buena y simple, se nos abre una multitud de dudas…

(12)Interesante buscar la referencia de Morten Bay, «What is Cybersecurity? In search of an encompassing definition for the post-Snowden era» (192), y si se quiere profundizar en el tema, una lectura a *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (193).

a) ¿Qué es, pues, el ciberespacio[13]?: si lo queremos resumir, internet y las entidades a través de internet (inter)conectadas.

(13)Aquí podríamos utilizar la definición de Ottis y Lorents del año 2010, de *ciberespacio*, «***cyberspace*** is a time-dependent set of interconnected information systems and the humans that interact with these systems». Y, por lo tanto, cuando hagamos referencia al ciberespacio, hemos de pensar en un entorno dinámico, en continua evolución, virtual, (inter)conectado y multinivel, de conceptos tales como la infraestructura física, los programas y aplicaciones (software), las normas y regulaciones, los procesos y las interacciones con las personas en todas sus formas (194).

b) ¿Cuáles son los activos a proteger en este entorno? Evidentemente, en un entorno de alta interconectividad (con los millones de dispositivos interconectados en un entorno IoT[14]), los activos son mucho más que la propia información: la infraestructura que dará soporte a la información (en un ámbito absolutamente global respecto a la implicada en los sistemas de computación, por la globalización en un entorno Cloud), y donde los propios protocolos de comunicación son de muy alta importancia (cómo comunicamos la información repercute en la seguridad de la información y, por lo tanto, no podemos obviar los conceptos asociados a las comunicaciones en ninguno de los planteamientos de ciberseguridad).

(14)Acrónimo para el término *internet of things*.

c) ¿Cómo manejamos o tenemos en consideración aquellos activos del ciberespacio que no son propiamente información?

d) ¿Cuántos ámbitos abarca la seguridad en el ciberespacio?

e) ¿Cuáles son aquellos aspectos de la seguridad de los sistemas de computación que permanecen cuando pasamos a hablar del ciberespacio, y cuáles aparecen como nuevos?

2) En su visión más global, la ciberseguridad se relaciona con la protección en un entorno de infraestructura crítica (redes energéticas, suministros de agua, salud pública[15], sistemas de transporte, redes de telecomunicaciones, servicios financieros, entornos industriales…) de todos los activos y agentes que están implicados para garantizar su confidencialidad, integridad y disponibilidad, de forma trazable y confiable.

(15)Podemos consultar, por ejemplo, «Privacy as a strategic advantage for healthcare products and services» (195).

3) Pero el aspecto realmente relevante de la ciberseguridad hace referencia a la conectividad. Todo está interconectado, y esta es la gran novedad… Ya no podemos considerar que nuestro entorno está aislado y, por lo tanto, blindado del exterior: tenemos unas fronteras, pero su permeabilidad ha crecido exponencialmente en tanto en cuanto los gestores de la información han de poder atravesar estas fronteras[16].

(16)En cualquier caso, no debemos confundir la no conectividad de los sistemas con la seguridad, ni obviamente la conectividad con la inseguridad. Sin ir muy lejos, el caso del malware Stuxnet, que llevó a la paralización de una planta de uranio en Irán, se llevó a cabo en un entorno sin conectividad a internet, pero con importantes vulnerabilidades que permitieron el ataque (162).

Cuando hablamos de seguridad, es importante que diferenciemos la seguridad de la privacidad. El concepto de privacidad está íntimamente ligado a los derechos inherentes de las personas. La privacidad de la información es un con-

cepto asociado con el derecho de disponer del control sobre la información personal de cada individuo, respecto a su uso, su recopilación y su gestión. La seguridad se centra en los tres aspectos básicos de la confidencialidad, la integridad y la disponibilidad de cualquier información, mientras que la privacidad se centra en la información personal y los derechos de los usuarios. Como hemos mencionado, hace referencia a la recolección de la información personal (qué puede recopilarse, cómo puede recogerse, quién puede acceder a la información recogida y cómo se podrá acceder a dicha información), pero también tiene que ver con la gestión de dicha información recopilada (cuándo, cómo y quién puede decidir que la información quede revelada a terceras personas o no, y en qué condiciones), pero además es relevante el uso de la información (no solo debemos considerar la información como personal, sino que no toda información podrá utilizarse para todos los usos).

El concepto de privacidad está, pues, íntimamente ligado con la normativa y la legislación, aspectos que desarrollaremos en el capítulo 5.

1.2. Estrategia de ciberseguridad industrial

1.2.1. Ciclo de gestión

Una vez hemos introducido algunas definiciones sobre seguridad, es el momento de pasar al ciclo de gestión de la seguridad. El primer punto es clarificar qué son activos (de los que ya hemos hablado anteriormente). Una correcta definición de activos hará referencia a algo que es valioso en una organización, como puede ser información, aplicaciones, servidores, equipos, bases de datos –nuevamente con información–, personas, edificios, infraestructuras… Es un concepto muy amplio. Si queremos verlo desde una perspectiva diferente, los activos serán todo aquello que hemos de proteger.

Los activos, como elementos a proteger, son vulnerables. Una vulnerabilidad representa una debilidad (un punto débil) de nuestros activos. Si tenemos activos, estos pueden tener puntos débiles, y estos representan marcas que indicarán (a terceras personas) nuestras debilidades, y por lo tanto, la potencialidad a ser atacados. Las vulnerabilidades pueden tener muchas caras, problemas de aplicaciones[17], versiones no actualizadas (de sistema operativo, *firmware*, aplicaciones…), defectos en políticas[18], o errores humanos.

[17]En inglés se suele utilizar el término *bug*.

[18]En inglés se suele utilizar el término *loop hole* para indicar que hacemos referencia a fisuras, vacíos legales, tecnicismos, que pueden conllevar debilidad en nuestros procesos que no parecen evidentes a primera vista (en derecho, este es un aspecto de gran relevancia cuando se redactan contratos, para el momento de un enfrentamiento legal, por una disputa, como podría ser un incumplimiento de contrato).

Las amenazas (que no debemos confundir con adversidades ni con ataques, aunque en algunos ámbitos o textos se intercambian los términos) hacen referencia a la potencialidad de aprovechar una vulnerabilidad. Sin vulnerabilidad

no podemos tener amenazas. Las amenazas pueden ser casuales (accidentales) o intencionadas. En cualquiera de los dos casos, dispondremos de la fuente de la amenaza, que suele tener dos vectores, el actor de la amenaza y la motivación de la amenaza. El actor puede ser una persona, un grupo de personas, una organización o incluso un gobierno. La motivación puede ser muy diversa, y puede estar asociada a los grupos de actores, o a los activos a los que se quiere amenazar: podría ser un tema de publicidad (renombre), fama, ganancias financieras, razones políticas o religiosas…

Pero, además del actor y de la motivación, en toda fuente de amenaza debemos considerar la capacidad[19], que nos indica el nivel de conocimientos y competencias, así como las herramientas y mecanismos necesarios para poder llevar a cabo la amenaza, y ser capaz de aprovechar la vulnerabilidad[20].

(19)En inglés se suele utilizar el término *capability*.

(20)En inglés se suele utilizar el término *exploit*.

Cuando las vulnerabilidades que existen en nuestro entorno quedan expuestas a sus amenazas, y pueden conseguir tener un impacto sobre nuestros activos, entonces tenemos los riesgos. El riesgo es uno de los puntos centrales en la gestión de la seguridad. Veremos cómo podemos modelarlo, y cómo podemos gestionarlo.

Evidentemente, ante los riesgos, que ya están donde nuestros activos, debemos aplicar controles y contramedidas para reducir el riesgo. Estas actuaciones, como veremos, pueden ir desde aspectos meramente tecnológicos a buenas guías (normalmente administrativas), políticas regulatorias (la Administración tiene un papel relevante en este aspecto)…

Pero, desde el lado opuesto (el del atacante), ¿cómo se perpetran los ataques? En los orígenes (los noventa), cuando todo empezaba, los atacantes utilizaban básicamente virus y gusanos para infectar los sistemas (y luego poder atacarlos), sistemas de comunicación (redes y protocolos) poco seguros (en aquellos momentos habían demasiadas comunicaciones sin cifrar…), o algo tan simple como configuraciones inseguras de los sistemas (podríamos decir que nos encontrábamos en los albores de la seguridad). Ante estos potenciales ataques, las contramedidas también eran claras (y en muchos casos simples): los antivirus, los cortafuegos (en las redes, para securizar los perímetros) y las guías de configuración segura (manuales en los que se indicaba lo que debía y lo que no debía llevarse a cabo con las configuraciones de los sistemas (en muchos casos meramente de los sistemas operativos, y los servicios que debían configurarse o abrirse). En algunos casos, se habla de estos primeros tiempos como de la «era de la protección». La seguridad se centraba en la gestión de la vulnerabilidad. De aquellos tiempos aprendimos que no puede plantearse ningún entorno sin tener en consideración la seguridad, y que la actualización de los sistemas (y de todos sus elementos) es el primer paso para poder aumentar nuestro nivel de seguridad.

Rápidamente se democratizaron los ataques. Es la época de los llamados *script kiddies*, o mejor recordada por la «era de los ataques en el lado del cliente». Ya nos encontrábamos inmersos en un mundo de aplicaciones cliente-servidor, en muchos casos funcionando (ya) en una base de navegador web (sino con una explosión de los entornos de *streaming* para las comunicaciones multimedia, o los entornos de mensajería[21]). Es el momento de desarrollar los entornos de escaneo y prueba automáticos, para detectar de forma rápida (en un entorno global) los sistemas vulnerables (y a veces incluso atacarlos de forma automática). Ante estos entornos la defensa pasa por la fase de defensa: se popularizan los IDS (sistemas de detección de intrusiones), los IPS (sistemas de prevención de intrusiones) y los SIEM (sistemas de gestión de eventos[22]).

(21)Los contenidos multimedia siempre son muy atractivos para el usuario final, y por lo tanto, siempre han sido uno de los focos de los atacantes para utilizarlos como vector de inyección de un ataque. Lo mismo sucede con los sistemas de mensajería, cada vez más instantánea, donde se suele utilizar por un lado la supuesta confianza en nuestro interlocutor (en aquellos primeros momentos sin ningún nivel de garantía sobre su autenticidad), o la supuesta urgencia de la comunicación, para poder atacar a las víctimas de forma sencilla.

(22)En inglés *security information and event management*.

No es suficiente aplicar medidas de prevención, hay que monitorizar y revisar de forma continuada, porque uno de los grandes factores de infección de nuestros sistemas viene por el lado de las personas (a veces, no se aplican las medidas de forma adecuada, o no se revisan y actualizan con la periodicidad necesaria, o simplemente se subestiman ciertas políticas, recomendaciones o situaciones de peligro).

(23)En inglés *advanced persistent threat*. Por ejemplo, nos puede ayudar el enlace de Imperva Incapsula Inc. (196).

(24)En inglés *distributed denial of service*.

Por lo tanto, el atacante ha ido evolucionando (y mucho): el ecosistema del atacante es muy maduro, y dispone de muchas (y muy sofisticadas) herramientas de soporte. Nuestra red se ha distribuido muchísimo, y tenemos unas fronteras muy difusas (lo que dificulta la defensa perimetral), ha aumentado el número de dispositivos interconectados (lo que aumenta las posibles fuentes de vulnerabilidades, amenazas, riesgos y ataques). Se trabaja en el ataque cada vez más de forma estructurada, pero sobre todo distribuida. Aparecen conceptos como APT[23] (mecanismos de ataque –*hacking*– que, de forma orquestada, van a estar continuamente probando y testeando un sistema, para finalmente encontrar el momento y la forma de atacarlo y comprometerlo), DDoS[24] (que buscan atacar o escanear sistemas de forma distribuida, para poder evitar así los controles de los sistemas de defensa, basados en la identificación de un potencial atacante, y el evitar que reincida, aunque no tenemos reincidencia individual, sino distribuida y controlada), las *botnets*[25](donde nuevamente dispositivos previamente atacados e infectados están bajo el control del atacante), proliferando para todos estos entornos las plataformas CC[26]; rápidamente nos adentramos en los conceptos (tan recurrentes actualmente) de *phishing*[27] o *ransomware*[28]. Es la era de la inmediatez, los sistemas de respuesta automática como los EDR[29] o los IAM[30].

(25)Abreviatura del inglés *bot (robot) network*.

(26)Abreviatura del inglés *command and control*.

(27)Para reflexionar sobre este concepto podemos consultar el informe *Internet Security Threat Report* 2017 (197).

(28)Interesante artículo de Kim Zetter en *Wired*: «What is Ransomware? A Guide to The Global Cyber Attack's Scary Method» (198).

(29)En inglés *end point detection and response*.

(30)En inglés *identity access management*.

Bienvenidos, pues, a nuestro punto de partida (y de interés): **la gestión del riesgo**[31]. Es la era donde están emergiendo las figuras (independientes) en las organizaciones del CISO[32]; debemos poner en el centro de la organización la gestión de la seguridad con todas sus consecuencias e implicaciones; por más medidas de seguridad que pensemos que tengamos, siempre podemos tener un punto vulnerable, todos somos atractivos al atacante desde un punto con-

(31)Es importante disponer de documentos actualizados con información sobre tendencias, por ejemplo, este informe de CISCO Systems Inc., *Cisco 2017 Annual Cybersecurity Report*, que requiere registro para descargarse, puede ser una buena fuente (199).

creto, y cualquier activo es de interés para algún actor. Las amenazas de seguridad se disparan, y la industria no siempre está preparada para seguir ese ritmo tan rápido, dinámico y dispar (recordemos el dicho de que el atacante no duerme… y nosotros estamos acostumbrados a trabajar de 9 a 17 horas). Es por ello que la defensa ha tenido (y tiene si no ha sido así) que evolucionar: hemos pasado de la protección (los cortafuegos) a la detección (los IDS, IPS), o a la gestión del riesgo (con un CISO y el despliegue de mecanismos de defensa y respuesta inmediata).

(32)Chief Information Security Officer, por encima del CIO, del CTO, o del CEO.

La gran pregunta de todas formas, siempre será la misma: ¿estaremos preparados para el futuro? Y, asimismo, ¿podremos dar respuesta a las amenazas y ataques del futuro?

La respuesta es complicada, pero si tenemos en consideración que:

1) desde la perspectiva del atacante[33], cada vez se tienen más ciberamenazas, no existe el concepto de perímetro (a securizar) (con la proliferación de los entornos de IoT (con el aumento de terminales finales) y las soluciones Cloud (con la distribución de nuestro entorno IT y un cierto no control directo sobre el mismo), y finalmente, el descomunal aumento de la capacidad de cálculo (y por lo tanto de ataque), y que

(33)Un rápido resumen de 5 puntos, en este vídeo de Dimension Data en YouTube, *Top 5 cybersecurity trends in 2017* (200).

2) desde la perspectiva de la defensa, debemos garantizar que daremos respuesta a los tres retos principales: la habitual falta de agilidad para actuar o reaccionar (nuestras organizaciones tienen muchas veces procesos, protocolos y entornos demasiado estáticos y muy poco flexibles, y por lo tanto debemos procurar aumentar nuestro margen de maniobra y actuación), la constante falta de presupuesto (la ciberseguridad seguramente no está en el lugar que le corresponde desde el punto de vista de inversiones, aún se suele ver demasiado lejos del negocio) y la evidente laguna competencial (hay una gran competencia por un mercado en el que el talento en la securización es muy limitado).

Si desde las organizaciones somos capaces de repensar nuestras estrategias (de forma integrada con el negocio, pero siempre teniendo presente la gestión del riesgo y de la seguridad), con la necesaria implantación de soluciones automatizadas (que sin duda son, y serán, cada vez más proactivas y preventivas), para poder dar el máximo con los recursos disponibles, y ponemos el foco también en la (re)formación de nuestros profesionales IT hacia el enfoque de la ciberseguridad, tendremos un gran camino ganado.

Pero no podemos cerrar este punto sin volver a dejar claro que el gran problema de la ciberseguridad siguen siendo las personas. La ciberseguridad no es meramente un problema tecnológico, y desde la perspectiva del CISO es imprescindible recordar en todo momento que las organizaciones son personas, y las personas son «débiles».

¿Cuáles son, pues, aspectos que hemos de considerar desde esta perspectiva? Vamos a nombrar algunos de ellos[34]:

(34)Pueden consultarse muchas fuentes con referencias, indicaciones y pautas, una de ellas podría ser la Agency for State Technology (AST) en Florida (EE. UU.) (201).

1) Ataques directos a la confidencialidad, que buscan al daño irreversible[35].

(35)Como podría ser, por ejemplo, lo que le pasó a Sony en diciembre de 2014, con la revelación de información privada y sensible.

2) Ataques directos a la disponibilidad, que buscan forzar la parada del negocio (el *ransomware* es el máximo exponente actual).

3) El perfeccionamiento de los mecanismos de ingeniería social.

4) El foco en la singularización (como en muchos entornos, la estrategia de defensa se basa en la detección, y esta en la repetición de patrones) no siempre es necesario ser muy sofisticado para poder atacar, sino imaginativo y único (y nos será fácil saltarnos los mecanismos de defensa).

5) No descuidar los canales tradicionales como fuente de ataque (el correo electrónico como uno de los principales), donde el *phishing* sigue siendo una buena estrategia para el atacante (es necesario invertir en el usuario final, en su formación, concienciación).

6) Sin duda, debe profundizarse (y mucho) en cómo utilizar la inteligencia artificial, el *machine learning* (o el *deep learning*) y, en definitiva, el concepto amplio de *big data* para reducir los retos en ciberseguridad. Desde esta perspectiva, es necesario considerar dos enfoques. Por un lado, el de los sistemas (que se van a autoconfigurar y gestionar, y que por lo tanto debemos garantizar que lo hagan de forma securizada), pero por otro lado, están los datos. En un mundo donde los datos, que luego se convertirán en información, serán el centro del negocio, un nuevo foco de vulnerabilidad pasa por la modificación de los datos[36].

(36)En inglés se utiliza el término *poisoning the data*.

7) Hemos de ser flexibles, y este será el eje central de las soluciones de seguridad. Es la era de la resiliencia[37]: como capacidad de recuperarse rápidamente de las adversidades para aprender a ser más fuertes y seguros. Para ello debemos garantizar que nuestros entornos, procesos y sistemas tienen la capacidad de recuperarse en tiempo (adecuado) a las adversidades (y aquí las soluciones de copias de seguridad[38] y de recuperación de desastres[39] en Cloud son el punto central), son ágiles –en tanto han de poder adaptarse de forma rápida y adecuada a las nuevas amenazas, cambios de entornos y necesidades del negocio (donde los entornos descentralizados, y nuevos conceptos como contenedores[40], los entornos de almacenamiento en Cloud, y el uso de tecnología basada en *block chain* para la descentralización, van a ser los elementos clave)–, están diseñados considerando la seguridad como elemento central del diseño (y aquí nuevamente tenemos toda una necesidad de formación en los desarrolladores, que va a ser fundamental para el éxito de nuestra misión).

(37)Interesante repasar el contenido de esta presentación: «Solving Cybersecurity in the Next Five Years: Systematizing Progress for the Short Term», de Sounil Yu, SVP Bank of America, en la *RSA Conference 2017*, (202).

(38)En inglés se utiliza el término *backup*.

(39)En inglés se utiliza el término *disaster recovery*.

(40)En inglés se utiliza el término *docker*.

Vulnerabilidades

En el ciclo de gestión de la seguridad, es necesario identificar nuestras vulnerabilidades.

Recordemos que podríamos definir una vulnerabilidad, por ejemplo, como una debilidad (una señal, un indicio) en un sistema o procedimiento de seguridad, diseño, implementación, control interno… que puede ser aprovechada, accidentalmente iniciada o intencionadamente explotada, resultando en una brecha de seguridad, o violación de la política de seguridad del sistema.

La forma de identificar vulnerabilidades puede ser muy diversa. Todos los esquemas (plataformas, soluciones) de gestión del riesgo ofrecen sus, digamos, propias metodologías para la identificación de vulnerabilidades. El punto de inicio, habitual, es una lista de vulnerabilidades estandarizadas, y un conjunto de áreas de control, a partir de las que trabajar, de forma conjunta con los propietarios de los activos afectados o personas con alto conocimiento del negocio, y de la organización.

Evidentemente, cuando se trabaja con vulnerabilidades, es bueno revisar de forma periódica y constante los portales de los proveedores de servicios de seguridad, o portales públicos, tales como la base de datos de vulnerabilidades de ICAT[41], NVD[42], CVE[43], portales CERT[44], listas de distribución[45].

Evidentemente, si disponemos de informes o auditorías de seguridad previas que se hayan llevado a cabo en la organización, deben ser el primer punto de partida. Demasiadas veces pasa que, cuando se vuelve a hacer una revisión de las vulnerabilidades de un sistema, se encuentran errores que ya fueron identificados en la anterior revisión y que nadie revisó ni subsanó.

Existen muchas herramientas para el escaneado automático de vulnerabilidades (que pueden ser utilizadas tanto desde la perspectiva del atacante como la del defensor). Su conocimiento y utilización es fundamental para todo gestor de la seguridad de una organización. Es el primer punto que va a utilizar un atacante sin demasiados conocimientos y, por lo tanto, debemos estar seguros de que no somos vulnerables a las herramientas de dominio público.

Por otro lado, deben utilizarse las recomendaciones (en algunos casos, las podremos considerar como requerimientos de obligado cumplimiento, por ejemplo, cuando se trate de los procedimientos de protección de las infraestructuras críticas que veremos en el capítulo 5.1) marcadas por los diferentes estándares de seguridad, que nos van a descomponer las posibles vulnerabilidades de nuestros activos en diferentes ámbitos: personas, hardware, software, información… Por lo general, las listas de control se estructuran en tres categorías:

(41) ICAT, «Identifying Critical Patches with ICAT Metabase» (203).

(42) National Vulnerability Database (204).

(43) Common Vulnerabilities and Exposures (205).

(44) Computer (Incident) Emergency Response Team.

(45) Como por ejemplo Security Focus (206).

- El apartado relacionado con los elementos de gestión: responsabilidades y gestión del riesgo.

- El apartado relacionado con los elementos operativos: protección de las infraestructuras, estaciones de trabajo, elementos de interconexión. Aquí deberíamos incluir también el correcto etiquetado (la señalética).

- El apartado relacionado con los elementos tecnológicos: criptografía, controles de acceso, identificación, autenticación, detección de intrusiones…

Si se trabaja de forma estructurada y ordenada, partiendo de unas listas iniciales, gestionaremos el riesgo en nuestra organización de forma consistente, entre diferentes episodios. Evidentemente, toda vulnerabilidad encontrada en el pasado debe ser revisada en todos los procedimientos de análisis posteriores (lo que nos permitirá reforzar nuestro grado de confianza en las contramedidas de seguridad implantadas en aquel momento).

Amenazas

En el ciclo de gestión de la seguridad, es necesario identificar nuestras amenazas.

Recordemos que las amenazas las podríamos definir como un elemento de aprovechamiento potencial de una vulnerabilidad específica por parte de un actor (de la amenaza) de forma accidental o intencionada.

Algunas de las amenazas que podríamos enumerar serían:

- Desastres (naturales).
- Fraudes.
- Oportunidad (aprovechar brechas, estar en el lugar adecuado en el momento adecuado).
- Dejadez.
- Descuidos.
- Terrorismo.
- Irresponsabilidad.
- Accidentes.
- Avaricia.
- Vandalismo.
- Sabotaje.
- Espionaje.
- Robo.
- Cansancio.
- Rutina.

Para poder manejar nuestros riesgos de forma adecuada, debemos ser capaces de identificar tanto nuestras posibles amenazas como sus fuentes.

Cuando hablamos de amenazas, solemos descomponerlas en tres elementos (componentes, factores):

- El origen de la amenaza.
- La tasa de ocurrencia (repetición) de la amenaza (su frecuencia): suele representarse en forma de probabilidad de ocurrencia.
- El impacto de la amenaza.

Algunas veces se utiliza la expresión de la ecuación siguiente, para cuantificar la amenaza:

$$ALE = V \times L$$

En esta expresión el término *ALE* hace referencia a coste anual de pérdida[46], *V* al valor del activo amenazado, y *L* representa la frecuencia de repetición (ocurrencia) de la amenaza.

(46)En inglés se utiliza el término *annual loss exposure*.

Ejemplo

Imaginemos un ejemplo sencillo de entender. Supongamos que tenemos, en Barcelona, un CPD, un centro de proceso de datos (en inglés se utiliza el término *data center*). Supongamos que un accidente natural que pudiera afectar la infraestructura (como podría ser una inundación, al estar cerca del mar) pudiera ocurrir una vez cada 100 años. Si valoramos el activo *V = 2 M*€, tendríamos que *L* = 0,01, y por lo tanto, *ALE* = 20.000 €.

El origen de las amenazas nos permitirá clasificarlas fácilmente en:

1) Amenazas internas: son aquellas que se originan desde la propia organización, teniendo un impacto normalmente mayor que las externas, precisamente por estar mucho más cerca de los activos afectados; además, el responsable del ataque (cuando es alguien de la propia organización, que no siempre es el caso) puede tener una información adicional de la propia organización, los procesos y los activos que puede ser muy relevante para el éxito posterior del ataque. La forma clásica de atacar este tipo de amenazas es mediante controles en las personas, procesos y sistemas de la organización, y mediante continuadas sesiones de formación y sensibilización: si todas las personas de la organización están continuamente atentas a todo aquello que pueda suceder que sea extraño, nuestro nivel de protección aumentará en gran medida (es la mejor defensa).

Podemos clasificar las amenazas internas sobre la base de:

- Accidentes.
- Usuarios con privilegios (sobre la información o los sistemas).
- Usuarios genéricos (sin privilegios sobre la información o los sistemas).

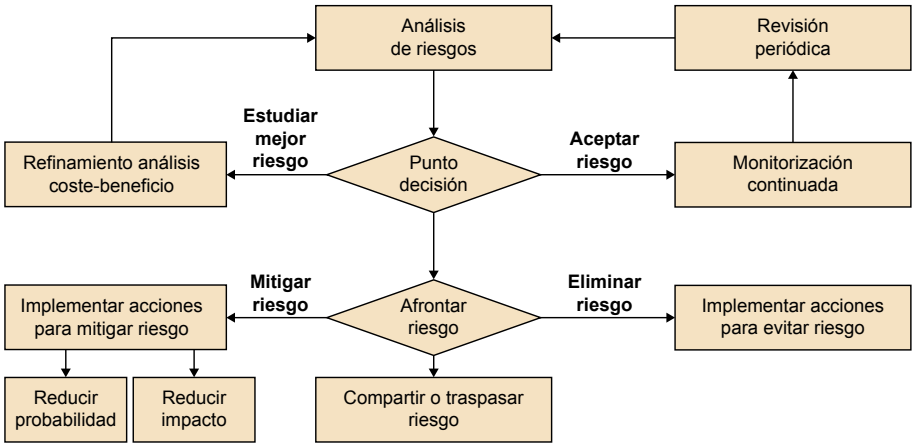
2) Amenazas externas: son aquellas que se generan desde fuera de la organización. Pueden ser dirigidas a un objetivo concreto y claro, o pueden ser genéricas (de tipo observador) buscando localizar vulnerabilidades no previamente identificadas. Una estrategia estándar de intentar mitigar estas amenazas es por procedimientos de seguridad perimetral, intentando securizar el acceso a nuestras instalaciones y sistemas, protegiendo los accesos.

Podemos clasificar las amenazas externas como:

- Intrusos.
- Programas maliciosos.
- Delincuencia electrónica.
- Virus informáticos.
- Troyanos.
- Ingeniería social.
- *Phishing*.

La puesta en marcha de un análisis coste-beneficio nos va a permitir disponer de un procedimiento consistente, comprensivo y estructurado para la identificación, estimación del alcance y selección de las soluciones para mitigar el riesgo sobre la base de una estimación efectiva del coste de la acción y del beneficio esperado, para llevar el riesgo a un nuevo nivel más adecuado para las operaciones de la organización.

Figura 4. Gestión continuada del riesgo



En la figura 4 vemos cómo podemos gestionar el riesgo:

1) Lo primero que necesitamos es disponer de métricas para tomar una decisión. Sin medir no podremos actuar.

2) La primera alternativa puede ser aceptar la situación de riesgo y, por lo tanto, no aplicar ninguna medida correctiva; simplemente, vamos a seguir monitorizando el riesgo, para garantizar que no salimos de la situación actual. Podría, por ejemplo, resultar demasiado costoso implementar ninguna medida respecto al beneficio que podríamos obtener; podríamos tener un impacto por debajo de lo que consideraríamos una situación de riesgo…

3) La segunda alternativa es demandar mejores métricas para tomar la decisión, por lo que debemos hacer un nuevo estudio del riesgo, las probabilidades de los impactos, de las vulnerabilidades, del valor de los activos… para volver a tomar la decisión. El proceso de generación de datos para obtener las métricas debe optimizarse y, en algunas ocasiones, se ha hecho de manera incorrecta o imprecisa y necesita una fase de refinamiento.

4) La tercera alternativa es hacer frente al riesgo y, por lo tanto, poner en marcha un plan de acciones. Este plan puede derivar en tres alternativas posibles:

a) Implantar un plan de acciones que eliminará el riesgo. Es muy difícil de conseguir y suele ser demasiado costosa (en todos los parámetros de valoración que pongamos sobre la mesa).

b) Implantar un plan de acciones que reducirá el riesgo. Es la opción más habitual. Se busca impactar en la probabilidad de éxito del ataque, o en reducir el impacto en caso de éxito. Cualquiera de las líneas de actuación mantienen vivo el riesgo, pero con una incidencia menor.

c) Implantar un plan de acciones que hará que el riesgo se derive a un tercero. Como no es fácil eliminar el riesgo, vamos a buscar que nuestro riesgo pase a ser el riesgo de un tercero, que ahora tendrá la responsabilidad de actuar sobre él. Es una medida que debe hacerse de forma controlada, pues no es evidente que un riesgo sobre un activo nuestro quede derivado. Un ejemplo claro sería traspasar el activo a un tercero.

Algunos parámetros que es conveniente que conozcamos son:

1) Previsión anual de pérdidas[47]: que será la base de un análisis cuantitativo, donde deberemos poder medir (cuantificar) el riesgo antes de las contramedidas, y después de su supuesta aplicación, y el coste del control (de esta forma tendremos el coste de nuestra actuación y el supuesto beneficio esperado de la misma).

[47]En inglés se utiliza el término *annual loss exposure* (ALE).

Ejemplo

Un ejemplo sencillo de entender podría ser el siguiente: imaginemos una plataforma de venta en línea que generase unos ingresos (beneficios) de 3.000 € por hora. Si esta tasa fuera constante, anualmente, los ingresos (beneficios) serían de 3.000 x 24 x 365 = 26.280.000 €. Si ahora tuviéramos la plataforma inoperativa durante 6 horas, podríamos calcular una estimación rápida de las pérdidas asociadas (representaría 6/(24*365) del total, es decir aproximadamente un 0,7 %. Las pérdidas indirectas, como podrían ser los

clientes potenciales perdidos, por ejemplo, son mucho más complicadas de estimar. En estos casos, es más fácil cuantificar los costes directos derivados de posteriores campañas de marketing y comunicación que los costes de pérdida.

2) Previsión de pérdida por un incidente[48]: en este caso, nos referimos a las pérdidas ocasionadas en el caso de que se produzca una sola iteración de la incidencia.

(48)En inglés se utiliza el término *single loss exposure* (SLE).

Algunas veces se utiliza la expresión de la ecuación siguiente, para cuantificar la amenaza:

$$SLE = V \times EF$$

Donde *V* es el valor del activo amenazado, y *EF* representa el factor de riesgo[49](el porcentaje de pérdida que podría sufrir el activo, en cuestión, en caso de una sola incidencia).

(49)En inglés se utiliza el término *exposure factor* (EF).

Ejemplo

Un ejemplo sencillo para entender el concepto sería: imaginemos que el activo es una finca, que valoramos en 300.000 €; imaginemos ahora que se produce un incendio en la finca y sufrimos unos daños en los que perdemos un 25 % de lo inventariado en ella. En este caso, *SLE* = 300.000 x 25 % = 75.000 €.

3) Tasa anual de ocurrencia[50]: hacemos referencia al número de veces que podríamos esperar, de modo razonable, tener una incidencia a lo largo de una anualidad. Evidentemente, este valor no es sencillo de estimar. A mejores datos y registros sobre actuaciones pasadas tengamos, mejor se podrá llevar a cabo esta estimación. Es una manera de estimar la probabilidad de una incidencia.

(50)En inglés se utiliza el término *annual rate of occurrence* (ARO).

De hecho, podemos volver a definir, de acuerdo con la expresión de la ecuación siguiente:

$$ALE = SLE \times ARO$$

Ahora tenemos la relación entre los tres términos que hemos definido. El parámetro *ALE* nos permitirá disponer de una referencia presupuestaria de lo que deberíamos invertir en medidas de seguridad para minimizar el riesgo de incidentes. Es un valor de gran importancia para el CISO de la organización. No hay seguridad absoluta, pero no hay ninguna seguridad sin inversión y este es un punto que, en algunos momentos, se menosprecia en algunas situaciones.

Ejemplo

Volvamos al ejemplo de los daños por incendio en la finca. Si estimamos *SLE* = 75.000 €, y *ARO* = 0,1, indicando que tenemos una probabilidad de tener un incendio cada 10 años, podríamos estimar *ALE* = 7.500 €, lo que equivaldría a la inversión que deberíamos hacer en la finca en medidas contra incendios.

Es muy importante, para todos y cada uno de los controles y actuaciones que tengamos definidos, tener una estimación de sus costes. Cuanto más detallados y desglosados los costes, mejor. Si conocemos el coste de adquisición, prueba, puesta en marcha, operación, comunicación, formación, monitorización y mantenimiento de cada una de las acciones, nos va a ser más fácil tomar decisiones respecto a la puesta en marcha o no de determinadas soluciones. Recordemos que la seguridad no es propiamente un fin, no es nuestro negocio en sí, sino que es una forma de garantizar que nuestra actividad se podrá desarrollar de forma correcta. No podemos (no deberíamos) gastar más en seguridad de lo que estamos protegiendo.

Aquí es donde vamos a introducir un nuevo concepto, el retorno de la inversión en seguridad[51], que viene a medirse sobre la base del valor estimado de *ALE* después de disponer de las contramedidas de seguridad respecto al mismo valor antes de las medidas. Si el coste de la inversión es inferior al retorno, hemos tenido doble beneficio (en medidas de seguridad, y en términos economicistas).

(51)En inglés se utiliza el término *return on security investment* (ROSI).

Ejemplo

Si tenemos evaluado el riesgo de incidentes en un servidor web con un *ALE* = 10.000 €; si implementamos unas medidas para reducir el riesgo que tienen unos costes anuales de inversión, operación y mantenimiento de 2.500 €, y con ello estimamos que ahora *ALE* = 2.000 €, podremos defender que tenemos un *ROSI* = 10.000 - 2.500 - 2,000 = 5.500 €.

Disponiendo de los costes de los riesgos (estimados) y de los costes de contramedidas, podemos empezar a pensar en el concepto de nivel de riesgo asumible. Como dijimos anteriormente, el objetivo de la organización es su negocio (su actividad) y, por lo tanto, desde la figura del CISO tenemos la responsabilidad de acompañar al equipo directivo y de gestión para que puedan entender los niveles de riesgo ante los que estamos haciendo frente, y cómo (en forma y nivel) un incidente de seguridad nos podría afectar. Al mismo tiempo, debemos tener la capacidad de poner sobre la mesa qué reducción podríamos tener en este nivel de riesgo, con qué aumento de la inversión en medidas de seguridad.

Ejemplo

Si disponemos de un equipo de seguridad, liderado por un CISO y todo su equipo, con grandes conocimientos tecnológicos, incluso de gestión, pero no son capaces de alinear sus actuaciones con el negocio, en tal caso, estaremos tirando a un saco vacío todas nuestras inversiones en seguridad, y no progresaremos en la dirección necesaria.

Evidentemente, en cuáles son los niveles de riesgo que podremos asumir, también tiene una gran importancia el marco regulador en el que nos encontremos. Recordemos que la gestión de la seguridad debe tener unos procedimientos claros, sencillos y eficientes para poder ser desplegados de forma eficaz. Al mismo tiempo, es importante no personalizar las situaciones de gestión del riesgo. No deben tratarse de forma individual ni individualizada las situacio-

nes. Un incidente de seguridad no es un problema individual, sino de todo un equipo, o de toda una organización. Cuanto más globalmente se responda a un incidente, mejor será la respuesta para esta situación y para las posteriores.

Al trabajar con amenazas es muy importante gestionar sus fuentes, los actores, pero también conocer (dejémoslo en prever) sus motivaciones. No vamos a tener que actuar de la misma manera si el atacante pertenece a un gobierno que si pertenece a una organización criminal organizada, o es un aficionado utilizando algún *script* que haya encontrado por internet[52], tal y como podemos ver en la tabla 1.

(52)En inglés se utiliza el término *script kiddy*.

Tabla 1. Actores, motivaciones y amenazas

Actor	Motivación	Amenaza
Script-kiddy	Curiosidad Ego	*Spoofing* *Hacking* de sistemas
Hacker interno	Ganancias económicas Desencanto	Fraude Documentación defectuosa
Cibercriminal	Beneficio Ideología	*DDOS* *Phishing* *Ransomware* Fraudes en tarjetas de crédito *Stalking*
Gobierno	Poder Revancha	Ataques a infraestructuras críticas
Personal poco formado	Errores no intencionados	Aceptar/introducir código malicioso Corromper datos
Cracker	Beneficio económico Modificar información	Ingeniería social Despersonificación de datos

Cuando sea capaz de tener listas de amenazas, revíselas de forma continuada, con equipos multidisciplinarios, que tengan una adecuada perspectiva de la organización, de sus procesos y sobre todo del negocio y sus activos. Si se trabaja la lista de amenazas, es conveniente manejarla cada vez que se debe enfrentar ante una nueva situación de riesgo, y procurar mantenerla lo más actualizada posible.

Para tener una idea de la magnitud del problema que nos atañe, podemos por ejemplo referenciarnos en el DBIR del 2015[53], donde vemos que se estimaron en 2015 unas pérdidas financieras de más de 400 millones de dólares, asociadas con más de 700 millones de registros de amenazas.

(53)Verizon (2015), *Data Breach Investigation Report* (DBIR) (207).

Evidentemente, para generar esta recopilación de amenazas, cada vez son de menor utilidad las listas[54], como mecanismo de identificación, detección y prevención de la amenaza. Cada vez van ganando más terreno lo que podría-

(54)La utilización de las llamadas en inglés *check lists*.

mos denominar servicio de gestión inteligente de amenazas[55] en forma de servicio o de herramientas para su uso. Se trata de disponer del conocimiento para tener la capacidad de identificar amenazas de forma automatizada, para generar a partir de ellas mecanismos de toma de decisiones automatizados y adecuadamente documentados. La gestión a la amenaza debe automatizarse cada vez más, para que el tiempo de respuesta sea cada vez más reducido. El componente de conocimiento (de inteligencia) siempre puede tener una doble perspectiva: por un lado, la meramente operacional (tecnológica) y, por otro lado, la estratégica (y de gestión más de comportamiento y no tanto de tecnología). El ámbito es muy complejo, pero no podemos dejar de invertir para obtener la respuesta adecuada en tiempo y forma, con una tasa de éxito cada vez mayor[56].

(55)Ver «Threat Intelligence Platforms: The Next "Must-Have" for Harried Security Operations Teams», Tim Wilson en *Dark Reading* (208) y Ed Tittle, «Comparing the top threat intelligence services» (209).

(56)Las metodologías utilizadas se basan en el término inglés TTP, *tactics, techniques and procedures*.

Algunas referencias sectoriales y globales podrían ser, en este ámbito:

- Financial Services Information Sharing and Analysis Center (FS-ISAC) (4).
- National Health Information Sharing and Analysis Center (NH-ISAC) (5).
- Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) (6).
- Retail Cyber Intelligence Sharing Center (RCISC) (7).

Cuando en el proceso de gestión de seguridad hemos llevado a cabo la identificación de amenazas y vulnerabilidades, deberemos llevar a cabo un proceso de vinculación[57] entre ambos. Es este un paso imprescindible para poder llegar al riesgo, entendido como la aplicación de una amenaza en una vulnerabilidad.

(57)En inglés se utiliza el término *TV pairing* (*threat-vulnerability pairing*).

Nuevamente, existen diversas metodologías y aproximaciones. Es obvio comprender que no todas las amenazas podrán aplicarse en todas las vulnerabilidades.

Un procedimiento sistemático que es relativamente simple de entender y de aplicar es el siguiente:

- Primero, se revisa la lista de vulnerabilidades, y se van apareando todas y cada una de las vulnerabilidades de la lista con todas aquellas amenazas con las que haya coherencia.
- A continuación, se revisa la lista de amenazas, para garantizar que todas y cada una de las que aparecen en la lista han sido asociadas con alguna vulnerabilidad.

En la tabla 2, podemos ver tres ejemplos de la relación, entre la amenaza, la vulnerabilidad (y una información relativa a una posible vía de explotación).

Tabla 2. Ejemplos de *TV pairing*

Vulnerabilidad	Origen de la amenaza	Actuación de la amenaza
Usuarios (nombres de usuarios) de personas que ya no tienen vinculación con la organización que no se eliminan de los directorios (*LDAP, Active Directory*).	Personal al que se le rescinde el contrato (en tiempo o antes de tiempo).	Podrían seguir teniendo acceso a la información confidencial de la organización.
La política de acceso del cortafuegos permite la conexión de entrada al protocolo telnet, y se ha dejado habilitado el usuario invitado en el servidor ABC.	Usuarios sin identificación en el sistema.	Se podría tener acceso a información del servidor ABC, accediendo al mismo a través de una conexión telnet con el usuario invitado (*guest*) (sin contraseña).
El desarrollador de una aplicación propietaria ha detectado/informado de problemas de seguridad, para los que aún no ha publicado los pertinentes parches de seguridad.	Usuarios no autorizados.	Sobre la base de la vulnerabilidad conocida, se podría tener acceso a información confidencial de la organización.

Riesgos

Al manejar el riesgo, como derivado de terceros factores, es importante tener herramientas y procedimientos para la correcta estimación de las probabilidades de ocurrencia de las amenazas (cuando se convertirán en ciertas) y, en tal caso, evaluar el impacto de la acción.

La consistencia en nuestro análisis del riesgo es muy importante. Es por ello que hay que procurar mantener un criterio estándar en la definición de las formas de medir la probabilidad de ocurrencia. Por ejemplo, puede utilizarse la siguiente gradación:

- Altamente probable (probable): el actor tiene una muy alta motivación, es adecuadamente competente, y los controles para prevenir la vulnerabilidad de ser explotada son ineficientes. Podríamos decir que tenemos un 76-100 % de posibilidades de que la amenaza sea exitosa en un año.

- Medianamente probable (posible): el actor está motivado, es competente, pero los controles de que se dispone deberían ser suficientes para impedir la explotación de la vulnerabilidad. Podríamos decir que tenemos un 26-75 % de posibilidades de que la amenaza sea exitosa en un año.

- Poco probable (improbable): el actor tiene poca motivación, o no es competente, y además los controles son los adecuados para prevenir y/o dificultar la explotación de la vulnerabilidad. Podríamos decir que tenemos un 0-25 % de posibilidades de que la amenaza sea exitosa en un año.

Es muy importante en esta triple clasificación dónde se van a fijar los umbrales. En el ejemplo que hemos descrito, la probabilidad de riesgo medio es el doble de la de riesgo alto-bajo. Pero podríamos fácilmente cambiar los criterios, si no lo consideramos adecuado para nuestro caso particular. Si por ejemplo tuviéramos los umbrales en 33 % y 66 % (en lugar de un 25 % y 75 %), la distribución sería mucho más uniforme en los tres niveles.

También podríamos, obviamente, aumentar el número de niveles, por ejemplo de tres niveles a cinco niveles: muy alto riesgo, alto riesgo, riesgo moderado, riesgo bajo, riesgo muy bajo.

Tomemos la decisión que decidamos, lo importante es:

- Consistencia, es decir, mantener las definiciones (a lo largo del tiempo, y las situaciones).

- Que exista consenso en su definición y uso, a lo largo de toda la estructura decisora de la organización, y que todo el mundo entienda los criterios de cada nivel.

- Que se documenten adecuadamente los criterios y niveles, y que se comuniquen.

Al mismo tiempo que se hace una estimación de la probabilidad del incidente, deberemos medir el impacto, en la fase de análisis del impacto.

El impacto lo podremos medir de forma cualitativa o de forma cuantitativa. Una forma muy simple de definir el impacto se basará en la pérdida o degradación de uno (o cualquier combinación) de los tres parámetros base: confidencialidad, integridad y disponibilidad. No se consideran todas las situaciones, pero es un buen principio, y es consistente y coherente.

Con la combinación de probabilidad y análisis del impacto, tendremos una cierta representación del riesgo.

Por ejemplo, en la tabla 3, podemos ver cómo se traslada la valoración de impacto y de probabilidad de éxito con la estimación de riesgo.

Tabla 3. Matriz de riesgo. Correlación de impacto y probabilidad

Riesgo		**Impacto**		
		Alto	**Moderado**	**Bajo**
Probabilidad	**Alta**	Muy alto	Alto	Moderado
	Moderada	Alto	Moderado	Bajo
	Baja	Moderado	Bajo	Muy bajo

De forma similar, en la figura 5 podemos ver cómo partiendo, por un lado, de la identificación de vulnerabilidades, amenazas y los controles existentes para la estimación de la probabilidad de éxito en el ataque, y por el otro lado, de la identificación de los activos, y la estimación de su valor, para poder valorar el impacto, podemos llegar a una adecuada estimación del riesgo. En nuestro ciclo de gestión de la seguridad hemos conseguido, pues, cerrar la primera de las tres fases: ya tenemos identificado el riesgo.

Nos faltaría describir dos niveles de detalle en la descripción (identificación, estimación) del riesgo:

- Nivel de cribado: nos va a permitir ordenar (priorizar) a grandes rasgos los riesgos (como sucede en un hospital cuando vamos a urgencias, en la sala de cribado). No se trata de afrontar el problema, se trata de disponer de herramientas y criterios para la priorización de las actuaciones. Estaríamos en una descripción básicamente cualitativa del riesgo.

- Nivel detallado: en este caso, dispondremos de información mucho más detallada del impacto, de las probabilidades, de los activos, de las vulnerabilidades, de las amenazas, de los actores, de sus competencias... Estaríamos en una descripción básicamente cuantitativa del riesgo.

Disponer de un nivel de aceptabilidad del riesgo[58] nos ayudará en nuestra toma de decisiones.

[58] Lo que podríamos definir como riesgo aceptable.

Si las comparamos, como vemos en la tabla 4, podemos ver que hemos de tomar decisiones entre el tiempo para la estimación del riesgo o la información para empezar las acciones de mitigación.

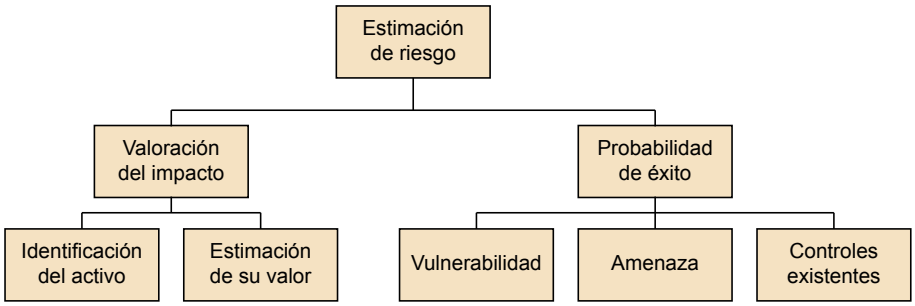
Tabla 4. Comparativa entre la descripción de cribado o detallada del riesgo

	Nivel de cribado	Nivel detallado
Pros	Rápido	Permite empezar a desplegar acciones de mitigación y suele permitir tener en cuenta los costes de las actuaciones.
Contras	Poca información para empezar con las acciones de mitigación (necesita de más detalle).	Se necesita mucho tiempo (y recursos).

Como en la gestión de las urgencias en los hospitales, en la gestión de la seguridad se está derivando hacia una política en la que se genera primero un nivel de cribado. Con esta metodología vamos a disponer de información sobre los riesgos, de forma lo más rápida posible, y ello suele conllevar una mayor eficiencia y eficacia en la gestión de los riesgos (se priorizan de forma sencilla, eficiente y efectiva, dando respuesta, siempre, a los casos realmente importantes).

Ahora tendremos que trabajar en cómo mitigar (reducir) el riesgo, en la fase 2, y finalmente perpetrar la monitorización continuada.

Figura 5. Estimación de riesgo, sobre la base de probabilidad e impacto



Ataques

El escenario al que nos enfrentamos para hacer frente a la posibilidad de un ataque es cada vez más complicado. Los atacantes cada vez están más preparados y, sobre todo, organizados; utilizan herramientas cada vez más potentes y, por qué no decirlo, cada vez más sencillas de utilizar, con lo que en cierta manera se está democratizando el ataque (cada vez puede atacarse mejor con menos conocimientos).

Cuando comparamos el ataque con la defensa, hemos de recordar que la motivación del atacante es muy alta, y que su éxito es total con una sola penetración[59].

[59]El atacante necesita un único acierto para tener éxito, mientras que el defensor debe ganar siempre, en cada uno de los envites.

La implantación global de soluciones móviles y en Cloud no ayuda para nada a la defensa, y permite una dinámica constante en los perfiles y orígenes de los atacantes. Cada vez es más habitual hablar de términos como *malware* polimórfico dinámico, ataques multivendedor, ataques multiestado, amenazas persistentes coordinadas…

No vamos a entrar en detalle en los procedimientos de ataque en este documento. Para una correcta evaluación de la resistencia a ataques de nuestra política de gestión de la seguridad es habitual contratar los servicios de una empresa (un especialista) de ciberseguridad que nos va a llevar a cabo un «ataque simulado» a través de una auditoría de seguridad (que puede empezar con un test de penetración).

1.2.2. Gestión del riesgo

Con los conceptos introducidos, podemos ya entender que la gestión del riesgo es un área multidisciplinaria, que ha estado activa durante años en sectores como el militar, programas aeroespaciales, teorías financieras, entornos de aseguradoras… Para manejarse en este entorno, es necesario entender conceptos de probabilidad, estadística y teoría de la información. Recordemos, pues, que habíamos identificado un riesgo como la existencia de una amenaza asociada con vulnerabilidades que podrían provocar daños (irreparables) a alguno de

nuestros activos. Por lo tanto, está claro que todo riesgo ha de tener asociados una amenaza, una vulnerabilidad y, claro está, un activo. Si nos falta alguno de ellos, podríamos decir que no hay riesgo, o mejor, que no podremos evaluar el riesgo. Si este activo no está adecuadamente valorado, no podremos gestionar el riesgo, pues no podremos evaluar la pérdida (que podríamos sufrir).

Como dice el dicho, «nunca tendremos un sistema plenamente seguro»; tendremos que vivir inherentemente con el riesgo.

Obviamente, el riesgo no indica certeza; por lo tanto, podríamos decir que el riesgo es la probabilidad de sufrir alguna pérdida (algún daño): interrupción de la actividad[60], pérdidas financieras, pérdida de privacidad, daños en la reputación, pérdida de confianza, consecuencias jurídico-penales…

(60)En inglés se utiliza el término *business disruption*.

Por lo tanto, cuando planteemos un sistema de gestión de la seguridad, debemos tener muy claro que nuestro objetivo no es la seguridad propiamente dicha, sino la gestión del riesgo. En este sentido, alguno de los errores típicos al plantear nuestro sistema de gestión de la seguridad es:

- Estudiar soluciones de seguridad sin tener claro el riesgo que nos afecta. Entonces, ¿seguridad para qué?

- Tratar riesgos que no afectan a la organización, o que son de los asumibles. En tal caso, ¿por qué gastamos recursos adicionales en reducir riesgos que no son relevantes? Dediquemos los esfuerzos a aquello que es importante.

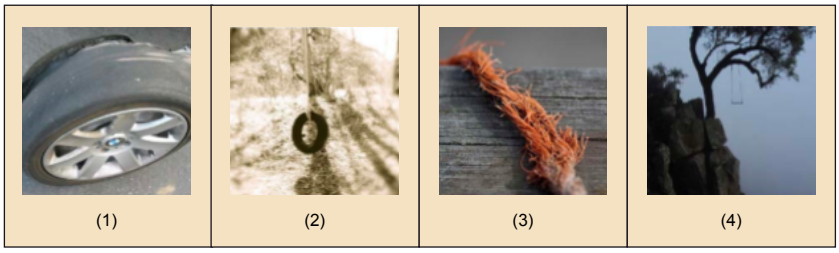
- Priorizar por costes o por facilidad de la solución. Ninguno de estos dos criterios suele ser el más apropiado. El objetivo no es recordar todas las acciones que se han implantado, como si el número fuera lo importante, sino reducir los riesgos que tienen impacto real sobre el negocio.

Aunque en el enfoque orientado a seguridad el riesgo está asociado mayoritariamente con aspectos negativos, puede tener consecuencias muy positivas: cuando sacamos un nuevo producto al mercado, cuando queramos abrirnos al mercado exterior, cuando vamos a adquirir algún activo, propiedad, negocio, compañía, bien…, evaluaremos también los riesgos, pero el resultado que buscamos será positivo; o incluso si vamos a cambiar, por ejemplo, nuestro ERP, evaluaremos también los riesgos asociados, pero el objetivo sería nuevamente, en principio, positivo.

Ejemplo

Como ejemplo para visualizar el concepto de riesgo (muy bien explicado por Philip Beyer (210)), me gusta mucho la visión del neumático liso, que presentan Jack Freund y Jack Jones en su magnífico libro *Measuring and Managing Information Risk, A Fair Approach* (8), representada en los cuatro escenarios de la figura 6:

Figura 6. Las cuatro imágenes del problema del neumático liso



«[...] The bullets below describe a risk scenario in four simple stages. As you proceed through each of the stages, ask yourself how much risk is associated with what's being described:

1. Picture in your mind a bald car tire. Imagine that it is so bald you can hardly tell that it ever had tread. How much risk is there?

2. Next, imagine that the bald tire is tied to a rope hanging from a tree branch. Now how much risk is there?

3. Next, imagine that the rope is frayed about halfway through, just below where it's tied to the tree branch. How much risk is there?

4. Finally, imagine that the tire swing is suspended over an 80-foot cliff with sharp rocks below. How much risk is there?

Now, identify the following components within the scenario. What was the:

- Threat,
- Vulnerability, and
- Risk?

Most people believe the risk is "high" at the last stage of the scenario. The answer, however, is that there is very little risk given the scenario exactly as described. Who cares if an empty, old bald tire falls to the rocks below? But, but…what about the person using the tire swing?! Ah, what person? We never mentioned any person.

Assumptions

Was our question about the amount of risk unfair? Perhaps, and we've heard the protests before…"But what if someone climbs on the swing?" and, "The tire's purpose is to be swung on, so of course we assumed that somebody would eventually climb on it!"

Both are reasonable arguments. Our point is that it is easy to make assumptions in risk analysis. In fact, assumptions are unavoidable because the world is infinitely complex.

That is our first point –assumptions are unavoidable. Assumptions are also the most likely source of problems within most analyses because, too often, people do not examine their assumptions or even recognize when they are making them. They just shoot from the hip. "That scenario is high risk!" they'll say. Unfortunately, the person next to them may be making a different set of assumptions and react with, "Are you nuts? Clearly that scenario is low risk!" Most of the time, the disagreement is based on different assumptions.

One of the significant advantages to using FAIR is that its ontology and analysis process help you to identify and clarify your assumptions. That way, when someone questions

your results, you are in a position to explain the assumptions underlying the analysis. [...]»

En cualquier caso, no hay que confundir vulnerabilidad con riesgo. Podemos imaginarnos detectar un servidor con una configuración errónea y enseguida podemos llegar a la conclusión de que estamos ante un riesgo elevado... Pero, en todo caso, lo que tenemos es una vulnerabilidad alta:

- ¿Existe correlación entre riesgo y vulnerabilidad? Claro que sí.

- ¿Es dicha correlación lineal? Claro que no, pues la vulnerabilidad, como hemos dicho antes, no es más que uno de los tres principales componentes del riesgo, conjuntamente con la probabilidad o la magnitud de la pérdida (activo).

Cuando hablemos de riesgo, será siempre importante que recordemos que se deriva de estos tres factores. El riesgo no es nada tangible, no lo podemos ver, no lo podemos tocar, ni tan siquiera lo podemos medir directamente. El riesgo es un valor derivado, como podemos ver en la figura 7, calculado, deducido, a partir de la combinación (resumiéndolo mucho) de la frecuencia de la amenaza, la vulnerabilidad y el valor del activo asociado.

Figura 7. Componentes del riesgo: amenaza, vulnerabilidad y activos

La gestión del riesgo es un proceso continuado, iterativo y dinámico donde, en todas y cada una de sus iteraciones, se puede descomponer en tres fases, que representamos en la figura 8.

1) Identificación del riesgo: en esta primera fase, el objetivo es la identificación del riesgo (es decir, de todos sus componentes): amenazas y vulnerabilidades, siempre en el ámbito de interés. Deberíamos poder identificar (en cierta forma cuantificar) el riesgo, a través de probabilidades o impactos. En esta primera fase, debemos tener una descripción comprensible del riesgo, cuanti-

ficar su impacto y ordenar (priorizar) a partir de su relación con la estrategia de nuestro negocio u otros condicionantes. Es obvio que para identificar el riesgo debemos proceder en tres subfases:

- Identificación de las vulnerabilidades; no solo las debemos identificar, sino que también las hemos de relacionar con nuestro negocio, para poder ordenar su posible impacto, sobre la base de los activos (y su valor) a los que pueden afectar.

- Identificación de las amenazas.

- Identificación de los activos (y su valor).

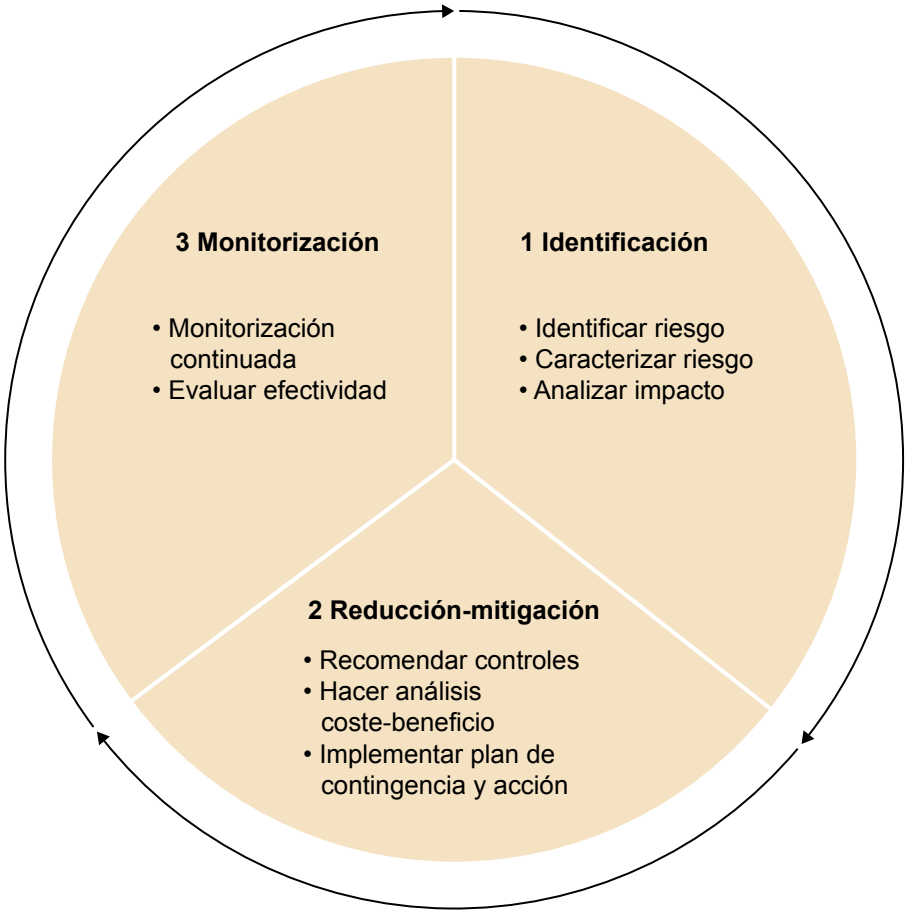
Esta fase de identificación es muy estructurada (metódica), y en lo posible debe automatizarse para poder hacerlo de forma reiterativa. Se suelen manejar conceptos claros y tipificados, así como matrices para llevar a cabo el proceso de registro (identificación).

2) Mitigación (reducción) del riesgo: con el proceso de identificación y priorización, pasamos a la fase de actuación, fase en la que implantaremos medidas (contramedidas) y controles para reducir (el impacto) de los riesgos. Es necesario poder establecer, para cada una de las actuaciones, su relación coste-beneficio (sin la cual no es posible implantar políticas, ni estrategias, ni evaluar los resultados). En esta fase, debe disponerse de políticas, procedimientos, guías, soluciones tecnológicas claramente redactadas, identificadas y documentadas, soportadas por las estructuras organizativas para su despliegue (tanto en los aspectos administrativos y jurídico-legales como tecnológicos o de gestión).

3) Monitorización del riesgo: después de identificar e implantar soluciones, debemos ver los resultados en una monitorización continuada que nos permita analizar la eficiencia de los controles y contramedidas desplegados. La cuantificación continuada nos va a permitir una mejora continuada de nuestra gestión del riesgo[61].

[61] Un buen referente para poder cuantificar las medidas que vamos a desplegar es SecurityMetrics (211).

Figura 8. Ciclo de vida de la gestión del riesgo: identificación, mitigación, monitorización



La gestión del riesgo puede enfocarse de dos formas:

1) Gestión reactiva: suele ser la solución utilizada cuando el número de incidentes (de seguridad) es reducido, y su impacto, digamos, menor. En este modelo, primero se produce el incidente (el mal, el impacto) y, a continuación, se despliega el procedimiento de respuesta. En primer lugar, se suele ir a reducir la afectación sobre el activo (contener el ataque), a continuación se procura identificar la causa (para dar respuesta y así procurar evitar repeticiones del mismo mal cambiando procedimientos, políticas, controles y configuraciones). En un escenario reactivo, suele ser conveniente no ir con prisas, pues cuanto mejor se actúe en un incidente, mejor se implantará la solución ante incidentes similares. Revisaremos las configuraciones de los sistemas implicados, los diferentes niveles y políticas de parcheo implantadas, los registros (*logs*) de todos los sistemas, el tráfico en la red de acceso a los sistemas afectados... para ser capaces de averiguar el origen del ataque.

Si no fuéramos capaces de mitigar el ataque en forma controlada en tiempo, deberíamos disponer de un plan de contingencia, de tal forma que deberíamos ser capaces de llevar a cabo las operaciones necesarias para nuestro negocio con el menor impacto posible. Debemos saber en qué forma nos impactará en el negocio.

Con el aumento de incidentes de seguridad, cada vez disponemos de más datos para poder, de forma estructura, perpetrar una gestión analítica de la seguridad a partir de datos registrados[62].

(62)En inglés se suele utilizar el término *data-driven security analytics*.

2) Gestión proactiva: en este caso el objetivo es la prevención, o dejar el entorno preparado para cuando en un futuro suceda un determinado incidente. Existen dos aproximaciones para caracterizar el riesgo: la cuantitativa y la cualitativa. En ambas, el objetivo es poder identificar amenazas y vulnerabilidades para determinar la probabilidad y el impacto de un riesgo concreto. Obviamente, esta no es una ciencia exacta, sino que está basada en aproximaciones (estimaciones). El procedimiento es predictivo, procesando una gran cantidad de datos (información) para, a través de su tratamiento, llevar a cabo una estimación de los riesgos asociados con determinadas operaciones.

a) Aproximación cuantitativa: es un procedimiento muy habitual en entornos financieros y de aseguradoras. Se suele asignar a los sistemas de información, procesos de negocio, costes de reconstrucción (de respuesta en marcha), y a partir de aquí, el impacto, y derivado de este el riesgo se va a medir a partir de costes directos e indirectos. Dispondremos de una muy precisa descripción del riesgo, pero antes de llegar a esta descripción los costes pueden ser muy importantes (incluso puede ser más importante la inversión para obtener la descripción cuantitativa que los beneficios que de ella se obtengan). Necesita muchas medidas, analizadas y procesadas por personal altamente cualificado. Por último, es importante recordar que estamos estimando y que, por lo tanto, una detallada descripción no tiene por qué coincidir con una correcta descripción. Dos soluciones típicas son las estimaciones de punto de riesgo o/y las distribuciones de probabilidad.

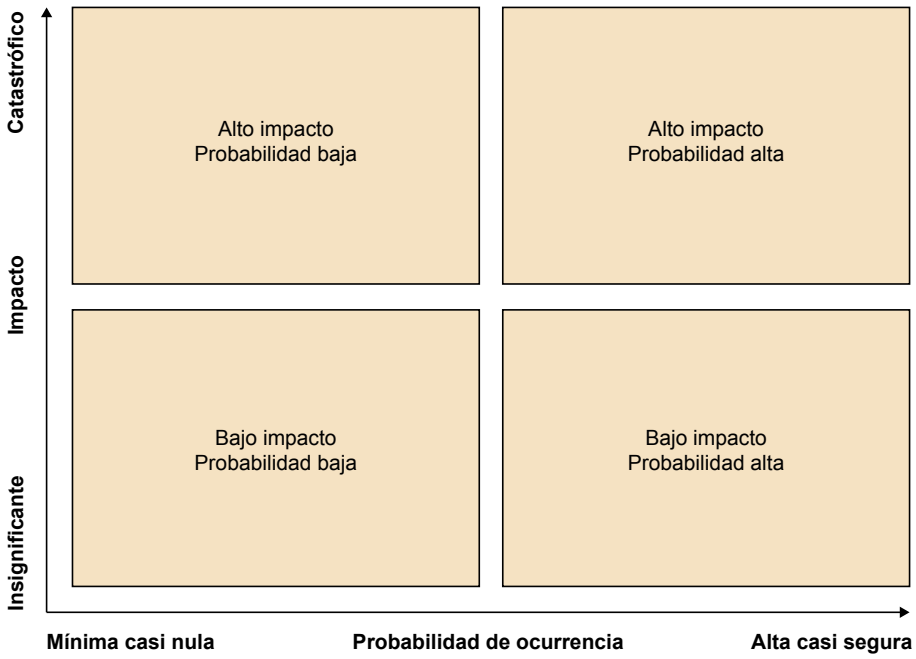
Cuando el riesgo está cuantificado podremos priorizarlo de forma sencilla, sea a partir de su impacto financiero (económico) o del valor financiero (económico) del activo (en cuestión), y de forma igualmente directa, podremos asociar un cierto retorno económico a la inversión en seguridad necesaria (tendremos una estimación de lo protegido). El mayor inconveniente es que el entorno que nos rodea es cada vez más global y que, por lo tanto, la cuantificación efectiva es cada vez más dificultosa. En definitiva, dificultad, tiempo, recursos, experiencia, costes…: demasiados condicionantes para que sea una solución normalmente efectiva y eficiente, por lo que, aunque sea una aproximación habitual en otros entornos o ámbitos, no suele ser habitual cuando se trata de gestión de riesgos en ciberseguridad.

b) Aproximación cualitativa: en este caso, ya partimos de saber que existe un alto grado de incertidumbre respecto a la probabilidad o el valor de los impactos, y por lo tanto se define el impacto, y el riesgo asociado sobre la base de parámetros altamente subjetivos (si se quiere, cualitativos). Se suele llevar a cabo una serie de cuestionarios y trabajos colaborativos para, a partir de ellos, extraer la información y los datos para la cualificación de los riesgos. Los grupos de trabajo han de ser multidisciplinarios y de perfiles, funciones

y categorías diferentes dentro de la estructura de la organización. Resulta más difícil presentar los resultados, pues la interpretación es mucho más subjetiva. Utilizaremos parámetros del tipo riesgo alto, moderado, o bajo para presentar los resultados, o escalas en el rango 1 a 5 (por ejemplo) basadas (casi siempre) en opiniones subjetivas, que transformarán la interpretación de la realidad en una escala subjetiva. Con ello se dispondrá de unas matrices (o tablas) con la información tabulada (en valores o colores) que puede ser adecuada para la presentación e interpretación de la información.

En muchos casos, tendremos matrices de riesgo como herramientas de presentación de la información, donde, en forma matricial, tendremos por un lado las probabilidades de que ocurra, y en el otro, el impacto si ocurriera (el ataque), como podemos ver en la figura 9.

Figura 9. Matriz de riesgo: probabilidad frente a impacto



Cuando hablamos de gestionar el riesgo, también debemos tener en consideración qué vamos a hacer con el riesgo (digamos identificado y/o cuantificado). Existen cuatro políticas generales de actuación:

1) Mitigación: suele ser la estrategia más habitual. Vamos a procurar poner en marcha contramedidas que compensen el ataque, reduciendo la probabilidad de que ocurra, o el impacto en caso de producirse de forma positiva. En esta línea de actuación, tenemos la instalación de parches y actualizaciones de sistema.

2) Transferencia: en esta estrategia, se traspasa a un tercero aceptar el riesgo en nombre nuestro (suele ser el caso de las aseguradoras). Es muy importante tener presente que traspasar (transferir) no tiene nada que ver con reducir

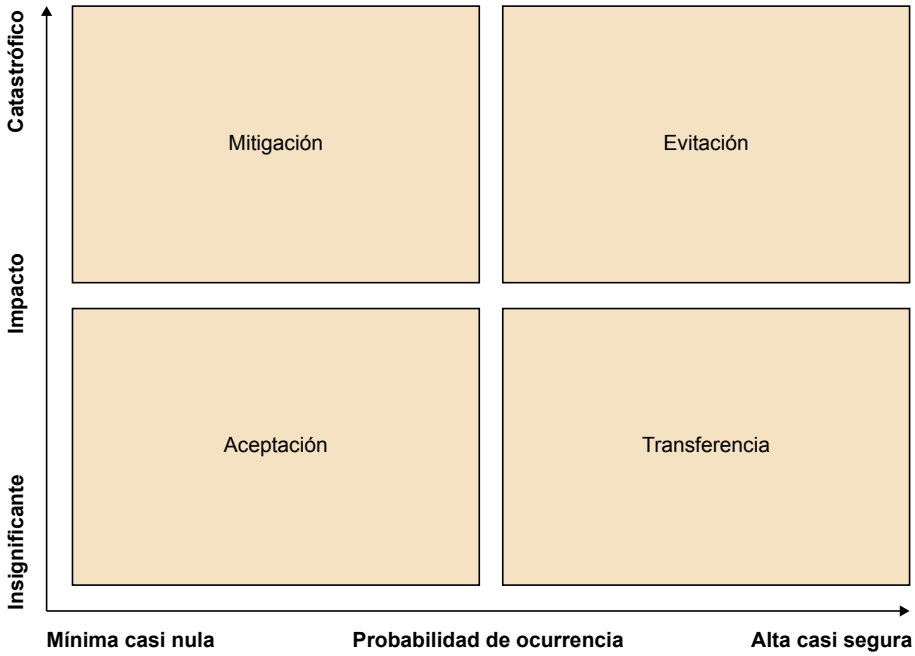
ni con mitigar. Lo que sí suele conseguirse es reducir el impacto del ataque (sobre todo, desde el punto de vista financiero). En este ámbito el concepto de ciberaseguradora está ganando presencia en el mercado.

3) Aceptación: admitiremos que el sistema (la organización) esté funcionando con un cierto riesgo (coexistiendo con el ataque). Muchos riesgos menores son simplemente aceptados. En otras situaciones en las que la mitigación del riesgo es demasiado costosa, lo único que se puede es aceptar el riesgo (en cualquier caso, como veremos más adelante, es imprescindible que este riesgo aceptable sea preaceptado por la cúpula directiva y gestora de la compañía). Si se ha etiquetado un riesgo como aceptable, la responsabilidad ante un ataque no debe ser del equipo técnico, puesto que fue la dirección la que aceptó el riesgo. Ha de quedar claro que la aceptación de los riesgos no corresponde al ámbito técnico de la compañía, sino al directivo (aquí podría/debería entrar en juego la figura del CISO).

4) Evitación: en esta última estrategia vamos a trabajar para eliminar los aspectos vulnerables que puedan provocar el riesgo. En algunos casos, se puede llegar incluso a eliminar el sistema (el activo) como única medida efectiva para evitar el riesgo. Es un ejemplo típico de este tipo de estrategias las asociadas con nuevas funcionalidades (servicios) que se puedan ofrecer: podríamos disponer de una plataforma web para que nuestros clientes puedan conocer el estado de sus pedidos. Imaginemos que la solución implementada permitiera que se pudiera acceder a la información de otros clientes, por un error en el sistema de autenticación de la plataforma, o por una incorrecta gestión de las sesiones de trabajo. En estos casos, a veces la solución efectiva pasa por la eliminación (suprimir) del servicio.

Como podemos ver en la figura 10, la forma en la que se suele gestionar el riesgo está íntimamente ligada con la matriz de riesgo.

Figura 10. Gestión del riesgo, en relación con su impacto y su probabilidad



La puesta en marcha de acciones y controles para mitigar el riesgo es una actividad continuada, y sistematizada, que debe ir haciéndose de forma recurrente sobre todos y cada uno de los activos de nuestra organización. Las acciones deben ir en dos líneas de actuación:

- Primero, reducir la probabilidad del incidente.
- Segundo, reducir el impacto en caso de éxito.

Normalmente, se trabaja en tres fases:

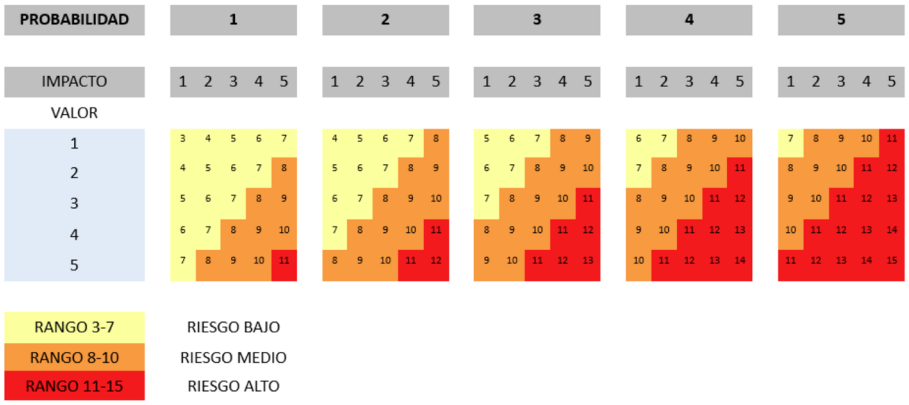
- Identificar controles recomendados que, normalmente, reducirán la probabilidad de éxito y el impacto.
- Realizar un análisis coste-beneficio para cada uno de los controles recomendados.
- Llevar a cabo una priorización de los controles.
- Diseñar e implementar un plan de acción (un plan mitigación) incluyendo, obviamente, tanto los aspectos de coste como los de tiempo.

Para la evaluación y representación del impacto en el negocio, suelen usarse (por su eficiencia) cuadros cualitativos, como los de las figuras 11 y 12.

Figura 11. Riesgo sobre el negocio como producto de la frecuencia y el impacto

MUY FRECUENTE 5	BAJO 5	MEDIO 10	ALTO 15	ELEVADO 20	MUY ELEVADO 25
FRECUENTE 4	MUY BAJO 4	BAJO 8	MEDIO 12	ALTO 16	ELEVADO 20
NORMAL 3	MUY BAJO 3	BAJO 6	BAJO 9	MIEDO 12	ALTO 15
POCA 2	MUY BAJO 2	MUY BAJO 4	BAJO 6	BAJO 8	MEDIO 10
CASI NULA 1	MUY BAJO 1	MUY BAJO 2	MUY BAJO 3	MUY BAJO 4	BAJO 5
↑ FRECUENCIA	**INSIGNIFICANTE**	**MENOR**	**MODERADO**	**ELEVADO**	**CATASTRÓFICO**
IMPACTO →	**1**	**2**	**3**	**4**	**5**

Figura 12. Riesgo como suma de probabilidad, impacto y valor del activo



En la primera fase, de identificación de controles, vamos a recopilar políticas, procedimientos y recomendaciones tanto operativas como tecnológicas. Existe un gran abanico de controles que podremos desplegar para aumentar la seguridad de nuestros activos. Los podríamos agrupar en las siguientes categorías:

1) Controles compensativos: suelen resultar como una solución alternativa a otras que son demasiado costosas y, por lo tanto, impracticables. En muchas situaciones estaremos cambiando una sola acción por una colección de acciones, quizás más simples, pero que nos permitirán caminar hacia la solución requerida.

2) Controles identificativos: que nos van a ayudar en la identificación de las actividades de un potencial atacante. En esta categoría, tendríamos todas las soluciones de sistemas de detección de intrusiones (IDS), los SIEM[63], las plataformas de gestión de amenazas[64], y cualquier solución de analítica de datos enfocada a seguridad.

(63)En inglés se usa el término *security information and event management*.

(64)En inglés se usa el término *intelligent threat management platforms*.

(65)En inglés se usa el término *disaster recovery*.

3) Controles de recuperación: que buscarán devolver nuestro entorno a la situación previa al incidente, normalizando las operaciones, como podrían ser las soluciones de *backup*, los sistemas de recuperación de desastres[65], o las soluciones respuesta a incidencias[66].

(66)En inglés se usa el término *incident response process*.

4) Controles correctivos: que arreglan y corrigen alguno de los componentes o sistemas después de un incidente. Por ejemplo, supongamos que debemos cambiar la política de control de accesos después de un incidente, y por lo tanto, debemos revisar los roles y los permisos.

5) Controles preventivos: que se van a desplegar para (intentar) evitar los incidentes. En esta línea de actuación tendríamos los sistemas de defensa (como los cortafuegos, las listas de control de acceso, los procedimientos de revisión de código y de programación segura, las unidades de testeo y control de calidad y seguridad, los controles para mitigar la posibilidad de intrusiones por errores de *buffer overflow* en nuestras aplicaciones, por vulnerabilidades de formato, o por inyecciones de código o comandos.

6) Controles disuasivos: que buscan desanimar a los potenciales atacantes. Puede ser algo tan simple como un cartel de aviso (el típico «cuidado con el perro», o «instalación protegida por central de alarma conectada 24 horas»), o los típicos mensajes cuando se accede a un sistema (a través de una conexión remota o directamente al sistema) que nos avisa de que podríamos hacer frente a procedimientos judiciales si entramos en un sistema al que no tenemos permiso de acceso.

Evidentemente, todos estos controles podrán implantarse de forma manual o de forma automatizada. Como ya hemos comentado, el equipo responsable de la gestión de la incidencia debe ser multidisciplinar, y debe poder evaluar (estimar) la efectividad de las soluciones (controles) propuestas. A lo largo de todo el proceso, deberemos ir documentado las medidas y su efectividad, para posteriores procesos similares.

Existen diversas tendencias para medir la efectividad de los controles. Una forma sería a través de cuestionarios, cada uno enfocado hacia una categoría de controles (trazabilidad, concienciación, comunicación, cumplimiento normativo, auditorías...). Por ejemplo, si hablamos de trazabilidad, haríamos referencia a las políticas definidas a tal efecto, para poder identificar las medidas que tenemos implantadas, y certificar su correcta operación.

El plan de acciones que vamos a desplegar[67], formará parte del informe que se debería remitir a la dirección de la organización. Es una herramienta estructurada para poder comunicar al equipo de gestión y dirección las acciones propuestas y su nivel de cumplimiento; nos indicará las recomendaciones, políticas, procedimientos y controles técnicos que hemos definido. En cada uno de los puntos, tendremos identificado la vulnerabilidad (riesgo) que vamos a

(67)En inglés se usa el término POAM, *plan of action at a milestone*.

procurar mitigar, las acciones/controles asociados, sus costes, los activos asociados, y el nivel de despliegue actual y futuro; asimismo, deberíamos disponer de una previsión temporal. Hemos de considerar el POAM como una herramienta de comunicación para la dirección de la organización mucho más que una plataforma de gestión propiamente dicha de la incidencia (no es una solución de gestión del proyecto, sino de comunicación del mismo). Ante una incidencia, se presenta una primera versión del POAM a la dirección que lo valida, y luego, durante toda la gestión de la incidencia, iremos reportando actualizaciones del mismo y el estado de despliegue de las acciones y controles previstos.

1.2.3. Métricas

El ciclo es claro y directo: solo podremos gestionar aquello que tengamos dimensionado (cuantificado), y solo podremos cuantificar aquello que tengamos clara y consistentemente definido. Por lo tanto, las métricas son conocimiento, pero para poder medir necesitamos conocimiento. Esta es una parte muy metódica del proceso de gestión de la seguridad, que puede incluso llegar a ser pesada y aburrida, pero que debe hacerse de forma continuada y muy rigurosa.

En procesos de negocio, es muy habitual hablar de indicadores de rendimiento[68]. Algunos indicadores podrían ser la rotación de inventario (como el número de renovaciones completas de un inventario anualmente), la tasa de conversión (en plataformas web, como el porcentaje de visitantes únicos a la plataforma que acaban comprando en el portal de ventas), el coste de suscripción para la adquisición (que representa todos los costes de promoción y descuentos revertidos contra el número de suscriptores finales, relación entre el aumento de suscriptores relacionados con las campañas de promoción y descuentos).

(68)En inglés se utiliza el término *key performance indicator* (KPI).

En la mayoría de indicadores, tendremos parámetros economicistas o de tiempo (que son fácilmente interpretables en forma de negocio directo de la organización). Este tipo de parámetros se procuran calcular de forma automatizada, para disponer de herramientas de control y de medida en el proceso de la organización.

Las matrices que utilizaremos para la estimación del riesgo deben procurar seguir recomendaciones y estándares, para mantener una consistencia más allá de nuestra organización, lo que nos va a permitir aprovechar la información de otras incidencias en otras organizaciones (que fueran medidas y trazadas de forma similar a como lo haríamos en nuestra organización). Con la matriz, lo primero que buscamos es facilitar la percepción de la situación; nos ha de permitir disponer de una foto del estado de nuestro nivel de riesgo, y de cuáles son los actores de riesgo más importantes, nos debe ayudar a entender cuán bien funcionan las contramedidas que hayamos podido implementar, etc.

Generamos (o podríamos generar) muchos datos alrededor del riesgo y la seguridad de nuestra organización, pero luego debemos ser capaces de analizarlos, para relacionarlos con nuestras operaciones de seguridad y con los propios procesos de la organización.

Cuando procuramos poner en marcha métricas en términos de seguridad, es importante que recordemos siempre que este es un proceso continuado; por lo tanto, cuando queramos conocer qué tal estamos, es conveniente que busquemos respuestas a preguntas del tipo:

- ¿Hemos mejorado nuestro nivel de seguridad (en este último ejercicio, después de la implantación de tal nuevo proceso…)?

- ¿Cuál es el impacto (beneficio) obtenido después de una determinada inversión en seguridad?

- ¿Cuál es mi estado respecto a estudios oficiales, respecto a mi sector…?

Cuando hablamos de métricas, hemos de recordar que hemos de diferenciar métricas de medidas. Las medidas nos permiten disponer de una visión en un momento específico en el tiempo, son valores discretos; por el contrario, las métricas tienen implícito el factor de comparación con un cierto punto de partida. Estamos hablando de dos o más medidas tomadas en diferentes momentos del tiempo. Las medidas comportan observación (conteo), mientras que las métricas incorporan un proceso de análisis. Las medidas son, pues, valores objetivos, de datos, sin ningún tipo de análisis ni tratamiento (son datos en bruto), mientras que las métricas tienen asociado un proceso de interpretación (deducido de un análisis) de los datos (que puede ser tanto objetivo como subjetivo).

De acuerdo con una buena categorización por parte de George Jelen (9) (de la International Systems Security Engineering Association) unas buenas métricas han de ser SMART:

Specific: concretas. Hemos de saber qué vamos a medir. Sin ninguna posibilidad de duda, porque, si no, la medida no sería un fiel reflejo de aquello que querríamos medir, y por lo tanto derivaría en una posible toma de decisiones equivocada.

Measurable: cuantificables (medibles). Si no podemos hacer una medida de ningún valor, la métrica no es adecuada; solo debemos tener en cuenta aquello que va a poder medirse, de entrada en este momento de forma teórica.

Attainable: asumibles. Estas medidas que teóricamente pueden efectuarse debemos estar habilitados para llevarlas a cabo en nuestra organización, con nuestros sistemas, con el personal y su capacitación del que disponemos, y obviamente con los recursos que tenemos a punto.

Repeatable: han de poder repetirse. Por un lado, para poder tener un conjunto de medidas, a lo largo de un cierto tiempo, que nos pueda ayudar a detectar situaciones de riesgo por comparación de históricos de las medidas, y por la capacidad inherente a un cierto método científico en la gestión de la seguridad, que puede requerir la repetición de ciertas medidas con valores, por ejemplo, almacenados en algún registro de nuestros sistemas, antes de la toma final de una decisión.

Time-dependent: variables con el tiempo. De forma que la medida esté en función del momento en el que se tome, y de las circunstancias propias de dicho instante.

Cuando hemos de definir un entorno de métricas para su despliegue en nuestra organización, es conveniente definirlo a través de proceso de mejora continuada, y en concordancia con otros procesos de la organización; no puede ser un modelo aislado del resto de procesos.

En cualquier caso, antes de desplegar cualquier medida de actuación, es conveniente ser realista. Debemos procurar siempre tener conocimiento de nuestra situación: cuáles son nuestras limitaciones, cuáles son nuestras fortalezas, qué información tenemos, qué objetivos tenemos, cuáles son los sistemas y procesos que tenemos, y cuáles dependen (y en qué medida) de nosotros o de terceros.

En esta misma medida, es muy importante tener muy bien identificados los recursos de los que disponemos para hacer frente a un incidente. Uno de los aspectos importantes es el referente a los recursos humanos. En muchos casos, este es uno de los aspectos más vulnerables de la organización. Es conveniente:

- Disponer de una clara descripción de las habilidades y competencias en términos de seguridad de nuestro equipo humano.

- Disponer de una clara planificación de disponibilidad de las personas.

- Disponer de una lista de personas y entidades de soporte (con sus competencias, disponibilidades y costes asociados) a las que poder recurrir en caso de necesidad. En muchos incidentes de seguridad el factor tiempo (de respuesta, de actuación) es uno de los factores más críticos.

- Tener claramente identificadas las personas y sus responsabilidades, en lo organizativo y operativo. Es importante tener identificadas y registradas

las identidades de las personas que llevan a cabo cada uno de los controles y procesos de nuestros planes de seguridad.

En este sentido, tenemos la relación de difuminación[69], definida como una forma de medida de la dispersión de responsabilidades. Es la relación de personal con responsabilidades operativas de seguridad sin pertenecer al equipo de seguridad propiamente dicho, respecto al total. Este factor de concentración también se puede aplicar a las personas externas a la organización respecto a las propias de nuestro equipo. Cuando este factor va creciendo, nos indica un mayor riesgo de seguridad.

(69)En inglés se utiliza el término *shadow ratio*.

Los costes en seguridad son otro de los aspectos relevantes y que debemos tener en todo momento claramente identificados. Estos pueden ser de tipo fijo, que no tienen dependencia con el volumen de la actividad, y otros variables, que se calculan sobre la base de volúmenes (de actividad, de personas, de transferencias, de operaciones, de clientes, de unidades de tiempo…).

Algunos costes fijos podrían ser:

- Costes de espacio (alquiler).
- Costes de depreciación (desvalorización).
- Seguros (de actividad, por ejemplo).
- Algunas licencias de aplicaciones (aunque a veces son variables).
- Componentes hardware de nuestro sistema, que se necesitan en principio independientemente de la actividad (por lo menos, son costes que tienen una variabilidad escalonada; por ejemplo, podemos necesitar un sistema de seguridad perimetral, que es independiente en cierta forma de la actividad, pues están dimensionados en un cierto rango de actuación).
- Los costes operativos (por ejemplo, de sueldos en personas relacionadas con el plan de seguridad).

Por su parte, algunos costes variables podrían ser:

- Las actividades de formación, que dependerán del punto actual (punto de formación actual del equipo), necesidades a corto, medio y largo plazos, incidentes identificados (potenciales o reales) de nuestro sistema de identificación de amenazas, vulnerabilidades y riesgos, servicios existentes o planificados…
- Capacidades de servidores o líneas de comunicación (y por lo tanto los costes a ellos asociados).

- Aplicaciones bajo demanda que podamos tener en funcionamiento.
- Servicios gestionados por terceras personas.
- Personal en servicio (*outsourcing*).

Se tome la política que se considere más adecuada, siempre deberíamos tener en cuenta los siguientes procesos:

Paso 1: Definir los objetivos del programa de métricas. Es importante recordar el considerable esfuerzo que puede suponer para la organización el hecho de trabajar sobre la base de un programa de métricas, y por lo tanto este esfuerzo (en tiempo, recursos, personas, inversiones…) debe estar claramente justificado. Lo hacemos para llegar a unos objetivos claros.

Podríamos, por ejemplo, trabajar con una métricas que nos indiquen de forma clara y simple cuán eficientes y eficaces somos en nuestra organización en cuanto al equilibrio entre los riesgos que podemos asumir y las medidas preventivas que podemos tener desplegadas, de tal forma que podamos dimensionar y justificar las inversiones en nuestro programa de seguridad, de acuerdo a nuestros objetivos de seguridad.

Estos objetivos de las métricas deberían ir acompañados de acciones de alto nivel, que deben desplegarse de forma global en la organización para alcanzar los objetivos marcados. A partir de la lista de objetivos se debería definir (enumerar) un plan de acciones, por ejemplo:

- Fundamentar nuestro programa de métricas de seguridad en la mejora continua de los procesos de nuestra organización.
- Apalancar, en algún proceso de la organización, cualquiera de las medidas que se tomen.
- Comunicar las métricas de forma adecuada para cada uno de los públicos a los que nos dirijamos. La comunicación no es nunca un proceso uniforme y monótono.
- Implicar a los agentes importantes de la organización en la determinación de las métricas que vamos a manejar. No puede nunca ser una decisión individualizada y alejada del negocio.

Paso 2: Decidir qué métricas deberemos gestionar. Aquí dependerá de nuestra línea de actuación. Si nos basamos en los procedimientos 6-sigma, nos centraremos en aquellos procesos de seguridad que buscan identificar errores (defectos, problemas) en procesos de la organización para su corrección, y por lo

tanto, en el momento de decidir qué métricas utilizar, lo primero que deberemos hacer será identificar aquellos procesos de la organización que pueden tener estos defectos de seguridad.

Si, por el contrario, nos centramos en una aproximación basada en el cumplimiento normativo, lo que buscaremos es nuestro grado de cumplimiento de las recomendaciones y mandatos de seguridad de los estándares. En este caso, lo primero será identificar cuáles serán los estándares que deberemos tomar como base.

Si no tenemos una metodología clara, siempre podemos atacar el problema desde las dos perspectivas clásicas:

1) Una aproximación descendente: hemos de intentar fijar los objetivos de nuestro programa de seguridad y, a partir de estos, descender para poder identificar las métricas específicas que nos podrían ayudar a obtener nuestros objetivos, y en todo caso, siempre nos permitan saber cuán lejos (o cerca) estamos de nuestros objetivos. Por ejemplo, podríamos:

- Definir una lista de objetivos globales de nuestro programa de seguridad: reducir el número de infecciones de virus en nuestra organización el próximo semestre en un 30 %.

- Identificar métricas que nos puedan indicar nuestro progreso hacia el objetivo final: relación actual entre las alertas de virus y las infecciones de acuerdo con el punto de referencia del ejercicio anterior.

- Determinar medidas necesarias para cada una de las métricas: número de alertas de virus en nuestra organización mensualmente.

2) Una aproximación ascendente: primero, llevamos a cabo la definición de los servicios, productos y procesos de seguridad que tenemos en la organización, que podrían o que ya son actualmente medidos. A continuación, determinamos cuáles podrían ser unas métricas adecuadas a definir sobre la base de estas medidas, y por último deberíamos poder determinar la bondad (eficiencia) de estas métricas con nuestros objetivos globales del programa de seguridad. Por ejemplo, podríamos:

- Identificar las medidas que están siendo (o podrían ser) tomadas para un proceso en concreto: número promedio de vulnerabilidades de primer nivel detectadas en un servidor de la organización, utilizando una herramienta concreta (y con una configuración concreta) de escaneado de vulnerabilidades.

- Determinar métricas que podríamos generar a partir de dichas medidas: cambios en las vulnerabilidades críticas detectadas en un servidor desde el

último informe (seguimiento del número de incidentes críticos de primer nivel en vulnerabilidades).

- Determinar la relación entre las métricas derivadas y los objetivos marcados globales del programa de seguridad: para poder reducir el número de vulnerabilidades detectadas en cada uno de los servidores de la organización.

La aproximación descendente es adecuada para la identificación de métricas necesarias de acuerdo a los objetivos globales del programa de seguridad, mientras que la aproximación ascendente suele derivar en las métricas más inmediatas (sencillas) de obtener. En ambos casos, eso sí, presuponemos que ya se han definido claramente los objetivos globales del programa de seguridad.

Paso 3: Desarrollar estrategias para la generación de las métricas. Cuando ya tengamos definido qué es lo que vamos a medir, debemos desplegar las estrategias (procedimientos) que utilizaremos para la recolección de información (datos) y de ellos derivar las métricas necesarias. Dichas estrategias deberán, en todo momento, especificar el origen de los datos, la frecuencia con la que capturaremos datos y la persona responsable de la captura: que los datos sean los oportunos, que las medidas se hagan en forma y tiempo adecuados, y que no se pierda la precisión (detalle) requerida con la captura; asimismo, deberemos definir el cómo y cuándo (y quién nuevamente es responsable) del proceso de tratamiento y análisis de los datos, para convertirlos en métricas.

Claras fuentes de datos; para esta fase son los *logs* (ficheros de registro de actividad) de cualquiera de los dispositivos de seguridad y programas y aplicaciones que tengamos desplegados. Disponer de una solución centralizada de *logs* nos va a permitir mejorar y optimizar esta fase del despliegue de la solución de seguridad.

Hay un buen número de herramientas disponibles para la automatización de esta fase del programa.

Paso 4: Establecer elementos de comparación (para evaluar): *benchmarking* es el proceso derivado de comparar, por ejemplo, el rendimiento y las prácticas (procesos) de defensa desplegados respecto a los de la industria (el sector de nuestra actividad), o lo que definimos como *best practices* generales. Comparando, vamos por un lado a ser capaces de disponer de un conjunto de nuevas ideas para gestionar nuestra actividad, pero por otro lado, y este quizás sea el punto más importante, vamos a disponer de elementos de comparación para poder disponer de métricas más interpretables, más justificables y, en definitiva, más útiles.

Nos va a permitir también establecer mecanismos que nos permitan dirigir nuestros pasos hacia una mejora continuada. Como responsables del programa de seguridad (por ejemplo, como CISO), debemos disponer de la información de referencia en el sector[70].

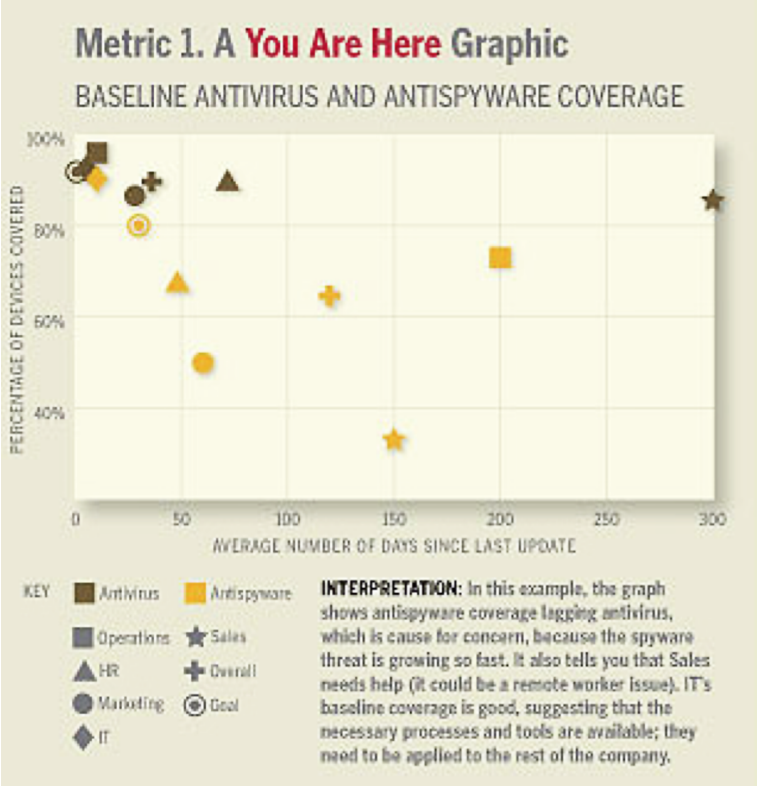
[70]Desde el punto de vista global, podríamos hacer referencia al portal CIO Magazine (213).

Paso 5: Decidir cómo vamos a informar del estado de las métricas: de nada nos sirven las métricas con las que estemos trabajando si no tenemos definido (y desplegado) un procedimiento de comunicación efectivo. Existen algunas referencias de cómo llevar a cabo este proceso (tan relevante en todo nuestro programa de seguridad). Hemos de personalizar la comunicación para cada uno de los roles en la organización y su grado de responsabilidad a los que vayamos a presentar los resultados. Las representaciones gráficas ayudarán mucho, y disponer de plataformas en línea (10), donde se pueda personalizar la información a visualizar (e incluso el cómo), es algo cada vez más común (el gestor ya no solo quiere disponer de la información, sino que quiere poder decidir qué información y de qué forma, o respecto a qué intervalo de tiempo analizar). Hemos de procurar que las métricas que utilicemos sean altamente comprensibles, y por lo tanto, a veces, es bueno no obsesionarse con aquellas que tienen una alta carga estadística y que uno piensa que nadie entiende. Las métricas que tienen menos carga teórica se fundamentan en la información que se puede extraer de nuestros ficheros de logs, del tráfico de nuestra red, del conocimiento de nuestros gestores de unidades de negocio.

Algunos buenos ejemplos en este aspecto podrían ser:

1) Seguimiento de nuestras herramientas de defensa respecto a algún punto de referencia, como podemos ver en la figura 13. Nos permite ver de forma rápida que está desplegado nuestro sistema defensivo, y nos permite garantizar que el grado de seguridad que vamos teniendo no se viene abajo, al tener una monitorización constante del mismo. Para poder disponer de esta información, es recomendable ejecutar escaneos continuados de nuestro sistema y generar las métricas de forma consistente a lo largo del tiempo.

Figura 13. Representación gráfica del estado de cobertura de nuestro entorno según los diferentes elementos de securización



2) Latencia de parches: nos indica con qué frecuencia instalamos y desplegamos parches en nuestros sistemas. Podemos tener información de los que se instalan, de los que cada vez que hacemos una actualización no habíamos actualizado…; en cualquier caso, es una forma rápida, si hacemos el seguimiento por máquina (sistema individualizado) o por tipo de sistemas, de garantizar que estamos dedicando el esfuerzo necesario para el despliegue continuado de parches y actualizaciones en nuestro entorno, y en qué puntos debemos mejorar nuestros procedimientos.

3) Robustez de las contraseñas: no se trata de desplegar las recomendaciones sobre las contraseñas (que siempre deben hacerse) respecto a la variabilidad, la longitud, la predictibilidad…, sino de probar si las contraseñas que tenemos en nuestro sistema son vulnerables. Nos hemos de situar en la piel del lobo y, utilizando herramientas de ataque de contraseñas, probar si las que tenemos son resistentes a estos ataques (digamos estándar). Es muy importante tener claro que el objetivo de esta métrica no es el usuario que acaba teniendo una contraseña débil, sino la seguridad de nuestro sistema. Si el usuario ha seguido nuestras recomendaciones (y no debería poder ser de otra forma), si la contraseña es vulnerable, el defecto está en las recomendaciones, no en el usuario. Si el usuario ha podido saltarse las políticas de contraseñas, entonces estamos en una situación aún peor, y debemos revisar urgentemente nuestros procesos de control.

4) Grado de rendimiento en nuestros sistemas: si de forma continuada vamos ejecutando herramientas de control en nuestros sistemas, que puedan ser consistentes y sistemáticas, podremos conocer el estado de los mismos, y en cierta forma compararlos con los referentes. Nos permite conocer sobre todo información respecto al hardware sobre el que estamos ejecutando nuestros sistemas. Es una forma de tener un ojo alerta sobre nuestra infraestructura, que nos avise de cuándo sería recomendable llevar a cabo renovaciones. No es tanto un tema de configuraciones como un tema de rendimiento.

5) Seguimiento del tráfico en nuestros sistemas (por ejemplo, del tráfico de correo electrónico): nos permitirá hacer un seguimiento de volúmenes (siempre en ambas direcciones, de entrada y de salida), de tamaños, de flujos (orígenes y destinos). Nos va a permitir detectar irregularidades en algunos usuarios que hayan podido tener sus cuentas de correo electrónico vulneradas, o revisar nuestras políticas de alertas en las herramientas de control que podamos tener desplegadas; nos va a garantizar que el sistema de correo electrónico no queda colapsado de golpe, pues podremos tener un seguimiento continuado de los usuarios, sus buzones y su actividad.

Las métricas que utilicemos no tienen que conocerse por parte de todos. Es obvio que hemos de tener definida una política de comunicación (a diferentes niveles organizativos y de responsabilidad), pero muchas de las métricas que vayamos a utilizar son de uso (y conocimiento) interno, por parte de los responsables de la seguridad de la organización.

Podemos disponer de unas métricas para informar (alertar) de situaciones y eventos, que nos han de permitir identificar una situación de riesgo y responder adecuadamente a tal situación, pero podemos, a partir de algunas métricas, derivar unas terceras métricas que son las que utilizaremos para hacer conocer cómo está funcionando nuestro plan de seguridad y poder justificar las contramedidas, acciones e inversiones en seguridad desplegadas.

Cuando trabajemos con las métricas que vamos a utilizar para la comunicación de nuestro plan de seguridad, y el seguimiento de nuestro grado de protección, es muy importante que tengamos presente que el objetivo último es la protección, y no conseguir que las personas, unidades y departamentos de la organización compitan entre ellos. No hemos de sacar los colores a nadie, hemos de disponer de los procedimientos y herramientas para mejorar nuestro grado de protección.

Las métricas son una forma de tener una información constante, consistente y actualizada de nuestra seguridad, y debe permitirnos sobre todo iniciar las acciones para responder ante una «nueva» situación de riesgo. Las métricas son para mejorar la seguridad de nuestra organización.

Paso 6: Crear un plan de acción y mantenerlo activo (y operativo): es el momento de la definición (enumeración) de todas las acciones con las que vamos a basar nuestro proyecto de seguridad. Tendremos métricas a tomar y comparar (analizar), fechas y frecuencias, acciones a perpetrar y alertas definidas.

No solo hemos de disponer de las acciones, sino que las hemos de relacionar con los objetivos de negocio de la organización. Cada plan debe estar alineado con la estrategia de negocio de la organización.

Paso 7: Establecer un ciclo de revisión continuado del programa: como en toda aplicación, el plan que definamos debe incluir una serie de medidas de revisión del mismo. Un plan que funcionaba hace unos meses no tiene por qué ser bueno actualmente, cuando podemos haber desplegado un nuevo servicio en la organización; puede haber aparecido una nueva vulnerabilidad (o amenaza, o riesgo), o incluso podemos haber tenido cambios en las personas y responsabilidades de las mismas en la organización, por lo que hemos de garantizar que el plan tiene un mecanismo de control y revisión continuado. Revisamos las métricas y las acciones para tener en cuenta el escenario cambiante que nos rodea. Disponemos de nuevas herramientas, que quizás debamos desplegar, de nuevos sistemas que hemos de poner en juego, y podemos tener nuevos servicios y procesos que debemos proteger. De forma continuada hemos de revisar nuestro plan desde un punto de vista de coste-beneficio, y hemos de revisar en qué y de qué forma estamos invirtiendo los recursos en seguridad en la organización.

La gestión de la seguridad es, ante todo, gestión, y, por lo tanto, se centra en la toma de decisiones. No podemos progresar sin ir desgranando alternativas y definiendo (y ejecutando) planes de actuación. Para todos ellos, necesitaremos un análisis coste-beneficio de las acciones a desplegar respecto a los beneficios en términos de seguridad que vamos (esperamos) obtener.

En esta línea, la ISO-17799 nos dota de un sistema de medida, equilibrado y comprensivo, que es la base en sistemas de gestión de seguridad de la información. Posiblemente, su mayor inconveniente radique en el hecho de una falta de concreción en la parte de definición, de conceptos clave, que pueden tener interpretaciones diferentes para diferentes analistas de seguridad.

Hasta hace no mucho, la situación en términos de incidentes de seguridad era la siguiente: las organizaciones que habían recibido ataques no hablaban de ello, para no ser desprestigiadas; por otro lado, aquellas que no recibían ataques no daban ningún detalle de cómo era su política de seguridad, para no poder desvelar ninguna información crítica (era la política del oscurantismo).

Evidentemente, el nivel normativo es muy importante para mejorar los niveles de seguridad, pues el nivel de riesgo por no cumplir una norma es mucho mayor que el de un posible incidente de seguridad. Pero no puede todo basarse en un alto nivel de burocratización.

Por otro lado, es obvio que la concienciación de la necesidad de inversión en seguridad también es una medida que va a ayudar a las organizaciones para aumentar su nivel de protección. Cuanto más seamos conscientes de lo oportuno de invertir en seguridad, y no lo veamos como un gasto en seguridad, mejor irá nuestro negocio.

Esta toma de decisiones, en un entorno de incertidumbre, puede atacarse siguiendo dos modelos básicos:

1) Una aproximación basada en modelos: podríamos decir que es una aproximación de arriba abajo, en la que se define un modelo para las amenazas, las vulnerabilidades, el impacto y, por lo tanto, para el riesgo. La idea es intentar disponer de un modelo que nos permita estimar los riesgos y, luego, intentar validar el modelo con los hechos.

2) Una aproximación basada en los datos: podríamos decir que es una aproximación de abajo hacia arriba, en la que buscamos basar nuestras decisiones de la experimentación a través de recopilar datos (por simple observación de los hechos) y a partir de datos (por procedimientos de análisis de series temporales de datos, o análisis estadísticos de correlaciones, seremos capaces de definir unas métricas).

La duda que siempre nos rodeará es cómo responder a la pregunta: ¿qué es una buena métrica?:

- Una buena métrica debe ser consistente[71].

- Una buena métrica no debe medirse solo por costes: no es tan importante lo que nos cueste obtenerla como lo que obtenemos una vez la tenemos. No es relevante si una métrica ha sido simple de obtener, si la información que nos da no es oportuna. Evidentemente, si podemos elegir, siempre es mejor una métrica rápida de obtener, fácil de obtener, poco costosa de obtener, y aún mejor si se obtiene de forma automatizada.

- Algunas métricas se podrán obtener de forma continuada, y otras deberán tener un proceso asociado que no nos va a permitir obtenerlas en tiempo-real.

- Las métricas pueden ser cuantitativas o cualitativas. Ambas son adecuadas y necesarias.

(71) Una buena métrica no debe ser (demasiado) subjetiva, y debe ser repetible.

- Las métricas deben estar contextualizadas.

- Las métricas deben ser lo suficientemente detalladas (precisas) para ayudar en la toma de decisiones (deben focalizar las alternativas para la toma de decisiones).

En el caso de la ISO 17799, por ejemplo, se define un procedimiento ordenado y estructurado, que descompone el problema de la seguridad de la información en una taxonomía de diez dominios (ámbitos) que van desde las políticas de seguridad a los controles de acceso físicos, o el desarrollo del sistema. Estos dominios en una segunda fase se descomponen en aproximadamente 150 áreas de control. Posiblemente, es una recomendación demasiado enfocada a la auditoría, y por lo tanto, peca de falta de recomendaciones más prácticas.

La parte de comunicación de las acciones que se puedan derivar de nuestro plan de seguridad y de las métricas que estamos tomando es muy relevante en todo el ciclo de gestión de la seguridad.

Hemos de poder, desde esta perspectiva de comunicación:

- Determinar qué es lo que vamos a presentar (qué información).

- Determinar cómo lo vamos a presentar (de qué forma, en qué formato).

- Determinar a quién se lo vamos a presentar (qué perfil, qué responsabilidad y qué conocimiento tiene).

- Determinar quién va a hacer la presentación (quién del equipo va a ser el encargado de la presentación a perfiles receptores diferentes; normalmente se asocian perfiles de presentadores también diferentes).

- Con qué frecuencia vamos a llevar a cabo la presentación.

- Cuánto tiempo va a durar la presentación.

- Qué documentación adjunta vamos a llevar a la presentación y vamos a entregar a la audiencia.

- Vamos a llevar a cabo un proceso de comunicación solo interno, o interno y externo.

- A través de qué medios vamos a llevar a cabo el proceso de comunicación externo.

Desde el punto de vista del CISO, la parte de comunicación del plan de seguridad, y de todas las métricas y acciones asociadas con él, es de vital importancia respecto a la dirección de la organización; en este sentido, es importante buscar en la presentación:

1) Complicidad con la dirección de la organización. No es nunca mi plan de seguridad, sino que ha de ser nuestro plan, y por lo tanto es muy importante que todo el mundo en el equipo directivo lo sienta como suyo. Es la única forma que puede ser llevado a cabo, y que los inconvenientes que pueda provocar en el normal funcionamiento de la organización sean aceptados por todos.

2) Repercusión. Es muy importante que aquello que comuniquemos llegue, y tenga un trasfondo que perdure mucho más allá de la propia presentación. Una forma muy eficiente de hacer comprender a todo el equipo la importancia de las acciones que se están presentando es presentar ejemplos reales. Si tomamos incidentes de seguridad reales y los trasladamos a nuestra propia organización, como si nos hubieran sucedido a nosotros, y ponemos sobre la mesa el posible impacto que podríamos haber sufrido en tal caso, es rápido, fácil y muy bien captado por la audiencia.

3) Transparencia. La seguridad nunca debe enfocarse como un tema a ocultar. Hemos de hablar de ella de forma clara y sin rodeos. Hemos de dejar claro cuáles son las acciones de nuestro plan de seguridad, para que toda la organización sea cómplice de ellas, pero al mismo tiempo hemos de dejar claro qué es lo que estamos invirtiendo, qué es lo que estamos protegiendo y cuáles podrían ser las consecuencias y repercusiones de un incidente de seguridad[72].

(72)Una lectura interesante en este aspecto sería la presentación «A Report from the Field: Implementing Cyber Security Metrics that Work», de Rick Grandy y Gregg Serene (214).

4) Límites de nuestro plan de seguridad. En esta línea, el equipo directivo de la organización debe conocer perfectamente hasta dónde podemos llegar en la defensa de nuestros activos, cuáles son los riesgos reales que se están asumiendo. El margen de seguridad con el que se va a trabajar depende mucho de la inversión que se va a poder asumir, y esta está directamente relacionada con el valor de los activos a proteger y el impacto de los posibles incidentes. Pero, en todo momento, hemos de conocer claramente la realidad de la situación. No podemos después encontrarnos con el «si yo hubiera sabido qué…».

5) Alineamiento con el negocio. El plan de seguridad no es un elemento aislado de la organización, sino que es uno más de los procesos que en ella se deben definir y desplegar para que la actividad principal de la organización tenga el mayor éxito posible. Si somos capaces de hacer ver que el plan de seguridad está acorde a la estrategia de negocio de la organización, nuestro camino por la senda de la gestión de la seguridad será mucho más sencillo.

6) Herramienta para la toma de decisiones. El plan de seguridad, en su alineamiento del negocio, debe disponer de las herramientas, mecanismos, indicadores y procedimientos oportunos para poder llevar a cabo la toma de de-

cisiones adecuada cuando se presenten las situaciones de conflicto, tanto si se ha producido un incidente como si se tienen que tomar decisiones de negocio, de servicios o de inversiones.

7) Adaptar el lenguaje al de la audiencia. La comunicación es fundamentalmente transferencia de conocimiento y, por lo tanto, el principal objetivo es que la audiencia entienda lo que queramos transmitir, no que sepan nuestras capacidades, competencias... El objetivo no es hablar de nosotros, sino que entiendan lo que estamos haciendo, y para qué, y la única manera de poder hacerlo es si hablamos en su idioma (y normalmente no el nuestro).

8) Directa. No debemos andarnos con rodeos. La seguridad (como la salud, si se quiere) no puede difuminarse, ni diluirse: la realidad es la que es y debemos enfrentarnos a ella siempre de frente, sin demasiados rodeos. Un incidente no debe minimizarse, una amenaza no puede menospreciarse, el impacto (real o posible) debe presentarse en su justa medida, porque es la única manera de poder afrontarlo y mejorar.

9) Utilizar hechos y datos en la presentación. Las evidencias (los acontecimientos) son fácilmente tangibles y, por lo tanto, comprensibles, y los datos serán los elementos que van a permitirnos aterrizar la presentación a nuestra realidad, con las métricas que utilicemos en todo el proceso.

10) Cuando queramos presentar las métricas y acciones de nuestro plan de seguridad, debemos priorizarlas. No siempre podremos (ni será conveniente) presentarlas todas, y por lo tanto es relevante decidir cuáles y cuántas.

Las herramientas de métrica tecnológica nos van a permitir la adquisición de datos, que luego podremos utilizar para la obtención y generación de otras métricas. Cuanto más precisas, detalladas y oportunas sean las métricas de ámbito tecnológico, mejor serán las que derivemos a partir de estas.

Tan importante es revisar la seguridad de nuestro entorno (nuestra red), analizando la defensa del perímetro, la cobertura de nuestras herramientas de defensa (hasta donde llegamos en cuanto a área de influencia), y aspectos de disponibilidad y control de la red, como hacer un análisis detallado de las aplicaciones con las que trabajamos, y hacer un adecuado seguimiento de las vulnerabilidades que podrían derivarse de estas aplicaciones.

Evidentemente, medir el grado de seguridad de las aplicaciones, muchas veces relacionado con el propio código de las mismas, es muy dificultoso. De entrada, no se ha establecido un criterio uniforme respecto a qué entendemos por una aplicación segura, con lo que ello dificulta aún más la evaluación de la seguridad de las aplicaciones.

Habitualmente, podríamos utilizar tres metodologías para medir la seguridad de las aplicaciones:

1) Métricas de caja negra: contaríamos los posibles flujos de ataque (de explotación de vulnerabilidades) de la aplicación tanto en local como en remoto, sin tener un conocimiento del código. Utilizaremos herramientas de escaneado de vulnerabilidades y, a partir de estas, iríamos contando las incidencias.

Podemos utilizar herramientas de escaneado o de test de penetración para la identificación de las vulnerabilidades. Una forma habitual de análisis es considerar una aplicación con posibilidad de acceso por el usuario vía remota (por ejemplo, a través de web), y entonces se analiza qué es lo que el usuario podría llegar a hacer, con toda una serie de acciones automatizadas de análisis (y ataque[73]).

[73]Algunas de las soluciones podrían ser SPI Dynamics (215), adquirida por HP en 2007 (216), Cenzic, adquirida por Trustwave en 2014 (217), Watchfire, adquirida por IBM en 2007 (218).

En los entornos web, se suele empezar por la URL de entrada a la aplicación, para luego identificar todas las páginas relacionadas con la aplicación, extrayendo los formularios que pueda haber, que suelen ser las fuentes habituales de vulnerabilidades. Lo que acabaremos teniendo como resultado es un indicador del número de vulnerabilidades, su tipología y su ubicación (en qué parte del ciclo de la aplicación). Normalmente se priorizarán en tres categorías (alta, media, baja) respecto a su riesgo (impacto), como herramienta de priorización para su posterior análisis y corrección.

Algunas de las técnicas frecuentemente utilizadas podrían ser:

a) Inyección SQL: se manipulan campos de formularios web, para poder obtener información sensible de las bases de datos a las que se ataca en el formulario.

b) Inyección de comandos: se intentan ejecutar comandos nativos del sistema operativo en el servidor web, a través del navegador.

c) Manipulación de parámetros[74]: se cambian parámetros de los formularios para intentar provocar cambios en el estado de la aplicación.

[74]En inglés se utiliza el término *tampering*.

d) CSS[75]: se busca que, ejecutando parámetros de entrada en formularios mal formateados que provoquen que podamos, a través de la ejecución de código malicioso de *scripting* (en JavaScript, por ejemplo), vulnerar sesiones de posteriores usuarios y así capturar datos sensibles de sus sesiones (como podrían ser las contraseñas de usuario, números de tarjetas de crédito…).

[75]En inglés se utiliza el término *cross site scripting*.

e) Desbordamiento de búfer[76]: se intentan sobrellenar zonas de memoria en el lado servidor, para provocar la caída del servidor, o para tomar el control del mismo, normalmente intentando tener acceso a alguna ventana de ejecución de comandos.

(76)En inglés se utiliza el término *buffer overflow*.

2) Métricas cualitativas, generadas a partir de indicadores estandarizados que hacen un análisis de los índices de riesgo de las aplicaciones. Basan el criterio en la frecuencia y calidad de los controles que se aplican al desarrollo de las aplicaciones.

De hecho, estas métricas que se pueden aplicar en diferentes fases del ciclo de desarrollo de las aplicaciones nos acaban dando pautas, indicios de lo que posteriormente podría ser una vulnerabilidad, por lo que tienen una gran importancia en la prevención de vulnerabilidades.

a) Revisiones de diseño: es bueno, en algún momento del diseño de la aplicación, incorporar criterios de seguridad en la revisión y hacer una revisión de las recomendaciones de los estándares de seguridad a este respecto.

b) Revisiones de arquitectura: debemos revisarla buscando puntos de vulnerabilidad, siguiendo las recomendaciones y estándares de seguridad a este respecto.

c) Revisiones de código: deben revisarse los controles que se han implementado en este aspecto. No se trata tanto de revisar sino más bien de auditar los controles ejecutados, pues recordemos que estamos en un análisis cualitativo.

d) Revisiones de herramientas automatizadas: identificando qué herramientas utilizamos para, por ejemplo, automatizar los test de penetración de las aplicaciones. No se trata de llevar a cabo el análisis, que correspondería con las métricas de caja negra, sino de conocer qué tenemos preparado y definido.

Todas las pautas e indicios que podamos encontrar en este análisis cualitativo deberán, posteriormente, poderse evaluar y calificar (en algunas categorías de riesgo, por ejemplo alto, medio, bajo). Si no somos capaces de hacer esta segunda fase en el análisis cualitativo, perderemos consistencia en el análisis, lo que dificultará mucho las acciones posteriores a la identificación de posibles vulnerabilidades, y, por lo tanto, perderemos entre otras cosas credibilidad en los datos que se deriven de nuestras métricas cualitativas. Debemos, pues, ser capaces de proceder a una estandarización de las definiciones y criterios que vamos a utilizar.

Algunos indicadores típicos podrían ser:

a) Medida del riesgo de negocio[77]: clasificaremos los posibles defectos de seguridad sobre la base del tipo de vulnerabilidad, el grado de riesgo y la estimación de impacto en el negocio derivado.

(77)En inglés se utiliza el término *business adjusted risk* (BAR).

Por ejemplo, es típico utilizar un BAR en el rango de 1 a 25, resultado de multiplicar dos factores, el impacto en el negocio (con un rango de 1 a 5, donde 5 indica un impacto significante) y el riesgo de explotación de la vulnerabilidad (también en el rango de 1 a 5, donde 5 indica un alto riesgo).

De hecho, es un parámetro que suele tener alta correlación con el ALE, que viene a calcular un concepto similar, pero utilizando herramientas y metodologías diferentes.

Algunos de los posibles inconvenientes del BAR podrían ser:

- Suele ser de rápida estimación, lo que le confiere poca precisión.
- En ningún caso se hace una cuantificación del riesgo en términos de tiempo o dinero.
- Los indicadores tienen una alta dependencia de los mecanismos de ataque (análisis) automático que podamos tener. Podrían tener algún riesgo muy alto, oculto, porque no esté en los canales de ataque «habituales».
- Los indicadores y resultados son claramente temporales. No debemos confiar en que un análisis hecho hace un cierto tiempo nos hubiera dado el mismo resultado actualmente, puesto que las herramientas y los vectores de riesgo podrían haber sufrido grandes e importantes modificaciones.

b) Índice de inseguridad de la aplicación[78]: donde no hacemos referencia a vulnerabilidades potenciales (lo que podría acontecer en el futuro, como con el BAR), sino que hacemos frente a afirmaciones simples y declarativas respecto a hechos que son reales, como podría ser que el servidor encripta los datos sensibles de la aplicación.

(78)En inglés se utiliza el término *application insecurity index* (AII).

Por lo tanto, nos focalizamos en una serie de cuestiones que acaban teniendo respuestas binarias (sí, no) que van a ser la base de nuestro indicador final.

Es una evidencia que es más fácil argumentar a partir de hechos que de suposiciones, como hacíamos en el BAR.

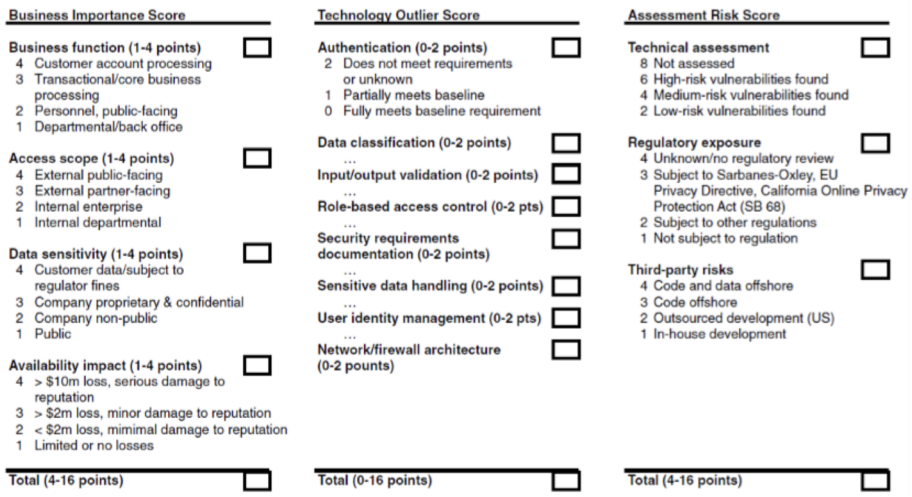
El resultado final no siempre tiene una relación lineal con el riesgo, pero nos da información muy valiosa. En algunos casos y entornos, se puede llegar a sacrificar una parte de la precisión de los indicadores para ganar en velocidad y, sobre todo, en capacidad de repetir los indicadores.

Se acostumbra a dividir estos índices en tres áreas:

- Relevancia en el negocio.
- Alineamiento tecnológico.
- Seguimiento global, sobre la base del riesgo y la normativa (fundamentalmente).

En la figura 14 podemos ver un ejemplo de cuestionario:

Figura 14. Ejemplo de cuestionario para evaluar el riesgo de inseguridad de una aplicación



Business Importance Score

Business function (1-4 points)
4 Customer account processing
3 Transactional/core business processing
2 Personnel, public-facing
1 Departmental/back office

Access scope (1-4 points)
4 External public-facing
3 External partner-facing
2 Internal enterprise
1 Internal departmental

Data sensitivity (1-4 points)
4 Customer data/subject to regulator fines
3 Company proprietary & confidential
2 Company non-public
1 Public

Availability impact (1-4 points)
4 > $10m loss, serious damage to reputation
3 > $2m loss, minor damage to reputation
2 < $2m loss, mimimal damage to reputation
1 Limited or no losses

Total (4-16 points)

Technology Outlier Score

Authentication (0-2 points)
2 Does not meet requirements or unknown
1 Partially meets baseline
0 Fully meets baseline requirement

Data classification (0-2 points)
...

Input/output validation (0-2 points)
...

Role-based access control (0-2 pts)
...

Security requirements documentation (0-2 points)
...

Sensitive data handling (0-2 points)
...

User identity management (0-2 pts)
...

Network/firewall architecture (0-2 pounts)

Total (0-16 points)

Assessment Risk Score

Technical assessment
8 Not assessed
6 High-risk vulnerabilities found
4 Medium-risk vulnerabilities found
2 Low-risk vulnerabilities found

Regulatory exposure
4 Unknown/no regulatory review
3 Subject to Sarbanes-Oxley, EU Privacy Directive, California Online Privacy Protection Act (SB 68)
2 Subject to other regulations
1 Not subject to regulation

Third-party risks
4 Code and data offshore
3 Code offshore
2 Outsourced development (US)
1 In-house development

Total (4-16 points)

En este caso, el rango de resultados estará entre 8 y 48 (en este caso, y es lo habitual, a mayor indicador, mayor riesgo). Vemos que se han categorizado las preguntas en los tres ámbitos que indicábamos:

- Respecto al negocio, analizamos los datos sensibles, temas de costes, temas de transacciones…
- Respecto a la tecnología, hacemos referencia a ocho diferentes ámbitos de aplicación (la categorización puede variar en cada cuestionario): autenticación, clasificación de datos, validación de entradas/salidas, controles de acceso basados en roles (perfiles), documentación de los requerimientos de seguridad, manejo de información sensible, gestión de las identidades de los usuarios, arquitectura de securización perimetral.
- Respecto al riesgo (11), se hace mucha referencia al aspecto normativo y de obligado cumplimiento de las aplicaciones[79], o todos aquellos riesgos derivados de terceros implicados, tanto en el desarrollo del código o en el almacenamiento de datos, y por último, se fundamenta en todas las acreditaciones que podamos tener, que den soporte y fortalezcan la securización de la aplicación.

[79]Como podrían ser las directivas de la Health Insurance Portability and Accountability Act de 1996 (HIPAA) (219) o de la Directiva Europea sobre privacidad (220).

Las preguntas, de hecho, sean las que sean, suelen en todos los casos:

- Dar las puntuaciones más altas a aquellas aplicaciones que son altamente vulnerables, que desatienden más las recomendaciones de los estándares de seguridad y tienen el nivel de incumplimiento más alto.

- Dar prioridad a aquellos aspectos que puedan obtenerse de forma fácil e inmediata a través de cuestionarios no demasiado densos y complejos de entender: ¿tiene nuestra aplicación transacciones de datos?, ¿tiene la aplicación conectividad exterior?, ¿maneja datos sensibles la aplicación?, ¿maneja correctamente los datos sensibles la aplicación?, ¿se gestionan los controles de acceso basado en roles?, ¿hemos efectuado controles de vulnerabilidades de la aplicación?, ¿tiene la aplicación código desarrollado por terceros?

- No incluir preguntas abiertas, del tipo ¿cuándo fue la última revisión de vulnerabilidades de la aplicación?, ¿qué controles de acceso tenemos habilitados?, sino que siempre son preguntas simples, con respuestas en lo posible binarias.

- No durar demasiado: el cuestionario tiene que ser breve. No se trata de preguntarlo todo, ni de querer averiguar información sobre todos los aspectos. Se trata de priorizar, para obtener la información adecuada, y de valor, y fiable.

3) Métricas basadas en el código, donde vamos a contar las incidencias localizadas en el código de las aplicaciones.

Algunos valores pueden ser:

a) Líneas de código[80]: que nos da una idea respecto al volumen, y, por lo tanto, también de la probabilidad de vulnerabilidades (en algunos casos se usan múltiplos tipo KLOC).

(80)En inglés se utiliza el término *lines of code* (LOC).

A veces, para simplificar y dar una idea de percepción similar, se cuentan las declaraciones del código (cuántos `if`, `for`, `while`, `calls`...).

En muchos casos, utilizamos herramientas de análisis automático de código, para detectar indicios de problemas como podrían ser RATS, ITS4 (*open source*), Klocwork, Coverity, Ounce Labs o Firtify software, que hacen énfasis en aspectos tales como la gestión (defectuosa) de memoria, la falta de validación en la entrada de parámetros por parte del usuario, o elementos del código que pueden nunca ejecutarse, o que pueden conllevar bloqueo de la aplicación.

La correlación de indicadores de cantidad (LOC) con los resultados extraídos de número de vulnerabilidades son los realmente importantes, para hacer frente a aspectos de seguridad de la aplicación.

Obviamente, todos los sistemas automatizados deben ser configurados a partir de criterios de falsos positivos y falsos negativos de la identificación. Suelen ser aplicaciones que no realizan una identificación y análisis sintáctico del código. En algunos casos, se hace un seguimiento de los flujos de ejecución de la aplicación, pero no buscan entender el código, y por lo tanto, aquí aún hay mucho camino por recorrer, pero no nos equivoquemos: la mayoría de grandes problemas vienen provocados por aspectos de codificación típicos y tópicos, que pueden identificarse a partir de la sintaxis de la codificación.

La gestión de métricas en nuestros proyectos de gestión de la seguridad tiene una alta relación con la gestión de la organización y son un elemento básico de comunicación con la alta dirección y de estrategia para hablar de seguridad.

La seguridad no puede, bajo ningún concepto, considerarse un aspecto aislado de nuestro negocio, y ya nadie lo considera como un conjunto de actuaciones a medida de los incidentes (y casi del momento y la capacidad de inversión), sino que se trata desde una aproximación holística[81] que comporta que se descompone en cuatro tipos de acciones (prevención, detección, análisis y respuesta) que operan como un todo, como un proceso unificado.

(81)Algunos autores presentan el término *programa de seguridad holístico,* como por ejemplo «Security Metrics Program – How it can help you get your senior management's buy-in!», ProServeIT Corporation (221).

Todo lo que maneje la seguridad desde una visión alejada de esta perspectiva global y unificada puede provocar el desperdicio de esfuerzos y recursos y la pérdida de tiempo.

Para que tengamos esta visión holística, es imprescindible la complicidad de la alta dirección de la organización, y de ahí el cada vez más importante rol del CISO en las organizaciones, como elemento de enlace de la seguridad con la alta dirección[82].

(82)Como refleja en su informe del 2015, el Ponemon Institute (un *think tank* de ciberseguridad americano) (222).

En la relación con la alta dirección, es relevante considerar los siguientes aspectos:

- Trabajemos de manera precisa nuestras métricas, para que nos permitan identificar qué está funcionando y qué debe mejorarse, y utilicemos este parámetro en nuestras comunicaciones.

- Acerquemos la política de seguridad al negocio, con lo que conseguiremos reducir la aversión hacia la seguridad de las direcciones habitualmente en nuestras organizaciones. Haciendo comprensible la política de seguridad, conseguiremos que la alta dirección le dé la importancia que tiene para el negocio.

- Las métricas deben utilizarse para responder a las dudas de la alta dirección. No solo están para trabajar mejor nuestro plan de seguridad, sino también para poder soportar y defender nuestros argumentos ante la dirección de la organización (los hechos derivados de las métricas son irrefutables).

En estos entornos, algunas de las métricas que podríamos derivar serían:

- La frecuencia de controles en el desarrollo de las aplicaciones: haciendo referencia a la rigurosidad de la unidad de QA[83] en nuestra organización (para los desarrollos propios), y qué pedimos para los desarrollos de terceros.

(83)En inglés se utiliza el término *quality assurance, quality assessment* (QA).

- El volumen de código, a partir de KLOC.

- La densidad de vulnerabilidades: que nos permiten obtener unos indicadores cuantitativos adecuados respecto a la seguridad de la aplicación y de su desarrollo. Unos de los principales aspectos de estos indicadores es que son claramente consistentes a lo largo del tiempo, y de todos los desarrollos que podamos llevar a cabo, pero por otro lado hacen referencia a la dificultad del posible ataque, no al impacto que se puede sufrir.

- Congruencia de las herramientas automáticas[84]: como métrica para calificar la bondad de las aplicaciones automatizadas de análisis de código. Se calcula como el número de problemas correctamente identificados, menos los falsos positivos, menos los falsos negativos, respecto al número total de problemas identificados. Es un parámetro de difícil cálculo, que debe realizarse por personal altamente cualificado y muy conocedor del código y de la aplicación.

(84)En inglés se utiliza el término *tool soundness*.

- Complejidad de las aplicaciones. Es obvio que la dificultad propicia la inseguridad, por lo que es adecuado tener un indicador de dificultad (complejidad). La complejidad ciclomática se define como el número mínimo de caminos que, en forma de combinación lineal, puede llevarnos por todos los flujos del módulo (de la aplicación, del código). Nos acaba considerando el número de ramificaciones de nuestro código, pero representa una métrica adecuada de complejidad.

Para finalizar con las métricas, podemos enumerar algunas de ellas en diferentes ámbitos de actuación, para disponer de una pequeña lista de referencia:

1) Planificación y organización

Riesgos gestionados:

- Porcentaje de activos (o funciones) que dependen de sistemas propios.
- Porcentaje de activos (o funciones) que dependen de sistemas de terceros.
- Porcentaje de activos (o funciones) que dependen de sistemas certificados.
- Porcentaje de activos (o funciones) que dependen de sistemas no certificados.
- Porcentaje de activos (o funciones) que dependen de sistemas con procedimientos claros de identificación de vulnerabilidades/riesgos/amenazas.
- Porcentaje de activos (o funciones) que dependen de sistemas con claros protocolos de documentación.
- Porcentaje de activos (o funciones) que dependen de sistemas identificados en nuestro plan de seguridad.

Recursos humanos:

- Porcentaje de personas con responsabilidades en seguridad.
- Porcentaje de personas con roles y responsabilidades definidas.
- Porcentaje de personas con certificaciones.
- Porcentaje de personas que han participado en alguna acción de mitigación de un ataque de seguridad.
- Porcentaje de personas que tienen responsabilidades de seguridad en la operación sin pertenecer al equipo de seguridad.
- Porcentaje de personas internas con responsabilidades de seguridad.
- Porcentaje de personas integradas en el equipo con responsabilidades de seguridad (sean internas o externas).
- Porcentaje (distribución) del equipo de seguridad en franjas horarias diferentes.

Recursos (presupuestarios)

Inversión en seguridad (puede medirse como medida absoluta, o como porcentaje respecto a otro valor del presupuesto, como podría ser el presupuesto total o el presupuesto en sistemas).

2) Adquisición y puesta en marcha

Identificación de procesos automatizados:

- Porcentaje de procesos con controles de confidencialidad (por ejemplo, en intercambios de información con colaboradores o clientes, o proveedores).
- Porcentaje de procesos con controles de integridad.

Identificación de procesos de securización. Son métricas que nos van a ayudar a conocer información de esfuerzo en seguridad derivado, directamente, de las consultas que en diferentes ámbitos recibamos. Cuando estemos en la operación de los servicios podemos seguir con las mismas métricas, pero ahora aplicadas a la operación.

- Porcentaje de actuaciones gestionadas internamente.
- Porcentaje de consultas externas realizadas en aspectos de seguridad.
- Porcentaje de consultas de seguridad por clientes.
- Porcentaje de consultas de seguridad por proveedores.
- Porcentaje de consultas de seguridad por colaboradores.
- Porcentaje de consultas de seguridad entre clientes, proveedores y colaboradores.
- Porcentaje de consultas de seguridad por unidades de negocio.
- Porcentaje de consultas de seguridad por servicio.
- Porcentaje de consultas de seguridad por sistemas, equipos…

Certificaciones:

- Porcentaje de aplicaciones certificadas (siguiendo algún estándar de seguridad).
- Porcentaje de servicios certificados.
- Porcentaje de procesos con certificación.
- Porcentaje de sistemas certificados.

3) Operativos

Formación:

- Porcentaje de cobertura por ámbitos de actuación en seguridad en nuestro equipo de seguridad (porcentaje de personas con unas competencias o conocimientos concretos).

- Porcentaje de personas del equipo de seguridad que han completado o recibido una formación concreta (o un proceso de certificación).

Sensibilización:

- Porcentaje de personas del equipo directivo que han seguido programas de sensibilización y formación en seguridad.

- Porcentaje de personas de la organización que han completado procesos de sensibilización (formación).

- Porcentaje de personas que han firmado determinados documentos o procesos de seguridad (por ejemplo, la conformidad respecto a la política de contraseñas).

Control de accesos:

- Número de identificaciones (de usuarios) asignadas a cada persona (identificación de personas con más de un perfil).

- Porcentaje de personas con acceso a determinados sistemas.

- Porcentaje de personas con acceso a aplicaciones de seguridad.

- Porcentaje de personas del equipo de seguridad que han sido revisadas (en sus perfiles y actuaciones).

- Porcentaje de activos con procesos de securización.

- Porcentaje de sistemas con procedimientos de bloqueo de cuentas de usuario.

- Porcentaje de cuentas de usuario con escalado de actividad (para identificar cuentas de usuario que deberían estar desactivadas, por ejemplo).

- Tiempo promedio para la eliminación de cuentas de usuario que deben ser eliminadas (tiempo de respuesta).

- Tiempo promedio para la desactivación de acceso a sistemas/procesos/aplicaciones para usuarios que han perdido el privilegio de acceso (por una degradación de roles).

- Tiempo promedio para la activación de acceso a sistemas/procesos/aplicaciones para usuarios que han ganado privilegios de acceso.

- Porcentaje de usuarios que han sido bloqueados por políticas de seguridad.

Imputación de costes:

- Porcentaje de gastos en seguridad por unidades de negocio.

- Porcentaje de gastos en seguridad por sistemas.

- Porcentaje de gastos en seguridad por servicios.

- Porcentaje de gastos en seguridad respecto a la inversión en sistemas.

Imputación de impactos en seguridad:

- Porcentaje de incidentes de seguridad por unidad de negocio.

- Porcentaje de incidentes de seguridad por sistemas.

- Porcentaje de incidentes de seguridad por servicios.

- Porcentajes de incidentes de seguridad con fuentes externas.

- Porcentajes de incidentes de seguridad con fuentes internas.

- Porcentaje de incidentes de seguridad por fallos humanos.

- Porcentaje de incidentes de seguridad por errores de configuración.

- Porcentaje de incidentes de seguridad por errores de parcheado de sistemas.

- Porcentaje de incidentes de seguridad derivados de procesos automatizados (deficientemente implementados).

Transferencias en las operaciones:

- Flujos de datos (en porcentaje) con clientes, proveedores, colaboradores, internos, de usuarios externos (en cantidad y en porcentaje).

- Porcentaje de toxicidad de datos (por ejemplo, definido como el porcentaje de registros con datos sensibles en las transferencias).

***Backup*:**

- Porcentaje de datos almacenados en sistemas de terceros.
- Porcentaje de operaciones de *backup* fallidas.

Privacidad:

- Porcentaje de dispositivos saneados antes de su uso.
- Porcentaje de incidentes de privacidad (confidencialidad) producidos.

Servicios operados por terceros:

- Tiempo promedio para revocar el acceso a sistemas corporativos a terceros que han perdido el privilegio de acceso a los mismos (por ejemplo, por cambio de proveedor de servicio).
- Tiempo promedio para dar acceso a sistemas corporativos a terceros que deben disponer de este privilegio (por ejemplo, para hacer frente a un incidente).
- Porcentaje de peticiones de acceso por parte de terceros concedidas positivamente.
- Porcentaje de peticiones de acceso por parte de terceros revocadas.
- Porcentaje de transacciones entre nuestros sistemas y los de terceros no autorizadas.
- Porcentaje de transacciones entre nuestros sistemas y los de terceros autorizadas positivamente.
- Acuerdos de operación con terceros con documentos claros respecto a los procesos de seguridad de la operación.
- Porcentaje de operaciones operadas por terceros.
- Porcentaje de usuarios de terceros de los que se han revisado los privilegios en un periodo de tiempo.
- Porcentaje de usuarios de terceros con incidencias de seguridad.

Gestión de la operación:

- Tiempo promedio para la implantación de cambios.
- Porcentaje de modificaciones derivados de alarmas de seguridad.
- Porcentaje de cambios derivados de excepciones y errores de ejecución.
- Número de cambios por implementar.
- Número total de incidentes detectados.
- Número total de incidentes operados.
- Tiempo promedio para la identificación de un incidente[85].
- Tiempo promedio para la identificación de vulnerabilidades (tiempo promedio entre vulnerabilidades).
- Tiempo promedio entre incidentes de vulnerabilidad.
- Tasa de incidentes de seguridad.
- Porcentaje de incidentes detectados por procesos de control automatizados.
- Porcentaje de incidentes de seguridad detectados por procesos internos de control.
- Porcentaje de incidentes de seguridad avisados por sistemas externos de aviso.
- Porcentaje de incidentes de seguridad identificados externamente a la organización (por el proveedor de algún servicio, como el de telecomunicación, por ejemplo).
- Tiempo promedio para recuperarse de un incidente de seguridad.

(85) En inglés utilizamos la métrica *mean time to know* (MTTK).

4) De monitorización

De proceso:

- Porcentaje de sistemas con procesos de monitorización implementados.
- Porcentaje de sistemas que ofrecen servicios a usuarios (clientes) con procesos de monitorización implementados.

- Porcentaje de sistemas conectados a internet con procesos de monitorización implementados.

- Porcentaje de sistemas con monitorización de la medida de varianza de su actividad (por ejemplo, por detección de un exceso de tráfico, o un exceso de peticiones de conexión).

- Porcentaje de sistemas críticos con revisiones asociadas a procesos normativos.

- Procesos de terceros con revisiones asociadas a procesos normativos.

- Porcentaje de controles con revisiones en sus procesos.

- Porcentaje de actividad de los controles (número de acciones controladas).

- Porcentaje de sistemas con incidentes de seguridad (alarmas de seguridad).

- Porcentaje de sistemas con incidentes de seguridad (alarmas de seguridad) críticos (graves).

De aplicaciones:

- Número de aplicaciones.

- Porcentaje de aplicaciones con incidentes de seguridad.

- Porcentaje de aplicaciones monitorizadas.

De usuarios:

- Porcentaje de usuarios con incidentes de seguridad identificados.

- Porcentaje de usuarios implicados en procesos vulnerables.

Normativos:

- Porcentaje de procesos de auditoría satisfactoriamente realizados (finalizados).

- Porcentaje de elementos pendientes de finalizar sus procesos de auditoría.

- Estimación de tiempo necesario para completar los procesos de auditoría pendientes de finalizar.

- Estimación de costes necesarios para completar los procesos de auditoría pendientes de finalizar.

- Porcentaje de procesos dependientes de terceros con procesos de auditoría satisfactorios.

- Porcentaje de procesos auditados con vulnerabilidades severas identificadas.

- Porcentaje de procesos auditados con vulnerabilidades medias identificadas.

- Porcentaje de procesos auditados con vulnerabilidades débiles (menores) identificadas.

- Tiempo invertido en procesos de auditoría (también puede medirse como porcentaje de tiempo invertido en procesos de auditoría).

- Coste de los procesos de auditoría (también puede medirse como porcentaje respecto a algún valor de referencia).

- Tiempo invertido en procesos de revisión (remedio) de situaciones vulnerables identificadas (o producidas) (también puede medirse como un porcentaje).

- Coste invertido en procesos de revisión (remedio/corrección) de situaciones vulnerables identificadas (o producidas) (también puede medirse como un porcentaje).

- Porcentaje de cumplimiento normativo (sobre la base de la norma, HIPAA; PCI, SOX...).

De parcheado:

- Porcentaje de sistemas con los parches actualizados.

- Porcentaje de sistemas parcheados en un determinado periodo de tiempo.

- Tiempo promedio para el parcheado de sistemas.

- Número (porcentaje) de vulnerabilidades críticas parcheadas en un periodo de tiempo.

- Número (porcentaje) de vulnerabilidades de riesgo medio parcheadas en un periodo de tiempo.

- Número (porcentaje) de vulnerabilidades de riesgo bajo parcheadas en un periodo de tiempo.

Gestión de vulnerabilidades:

- Tasa de falsos positivos.
- Tasa de falsos negativos.
- Porcentaje de sistemas monitorizados.
- Porcentaje de equipos sin ninguna vulnerabilidad severa identificada en un periodo de tiempo.
- Porcentaje de sistemas sin ninguna vulnerabilidad severa identificada en un periodo de tiempo.
- Tiempo promedio por vulnerabilidad invertido en sus procesos de mitigación.
- Tiempo total invertido en procesos de mitigación de vulnerabilidades.

1.2.4. La seguridad a partir de datos

Una forma de atacar la gestión de la seguridad, cuando se dispone de los recursos (en buena parte humanos adecuados), es partir de los datos que nos rodean para con ellos obtener la información que nos permita operar.

Los ingenieros conocemos la base de las teorías desarrolladas por Claude Shannon (12), que han derivado en la ciencia de la teoría de la información: en ella, definía la información como la cantidad de reducción de incertidumbre en una señal, que se podía relacionar con la entropía que se había podido eliminar de la señal. En su teoría siempre disponíamos, como receptores de la información[86] siempre de un cierto nivel de incertidumbre que debía reducirse con la información transmitida; medía niveles de información que podían transmitirse en una señal, el nivel mínimo que debía tener una señal para poder hace frente al ruido, o la máxima compresión que se podía aplicar a los datos, para no perder información.

[86]Hemos de pensar que sus teorías estaban originalmente muy enfocadas a los canales de comunicación, con un emisor y un receptor que iba a recibir una cierta información.

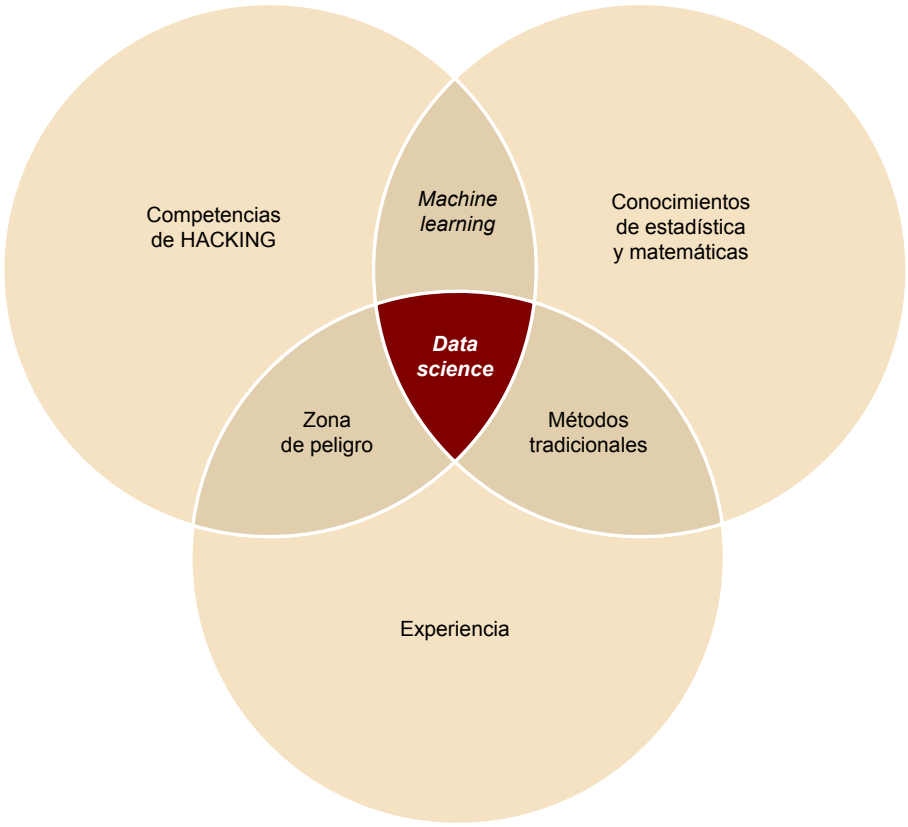
Este concepto de reducción de la incertidumbre es el elemento clave de la teoría de la información que es aplicado en las situaciones de análisis de riesgo, para poder tomar decisiones de forma estructurada y analítica: los datos que nos van a servir para la toma de decisiones son información, basada en observaciones empíricas que nos proveen de una evidencia cuantificable que redu-

ce nuestro nivel de incertidumbre. Con estos procedimientos tan analíticos se elimina todo factor subjetivo de la toma de decisiones, que queda fundamentada en una ciencia exacta.

A partir de estos datos y su análisis[87], con herramientas de *machine learning*, *data analytics* y *artificial intelligence*, podemos en el campo de la ciberseguridad extraer información para los modelos de gestión del riesgo, en forma de amenazas, vulnerabilidades, impactos, factores coste-beneficio, que nos van a permitir diseñar nuestra toma de decisiones en todo el proceso de gestión del riesgo (identificación, mitigación evaluación continuada).

(87)En inglés se suele utilizar el término *data-driven security*.

Figura 15. Diagrama de Venn de *data science* de Drew Conway



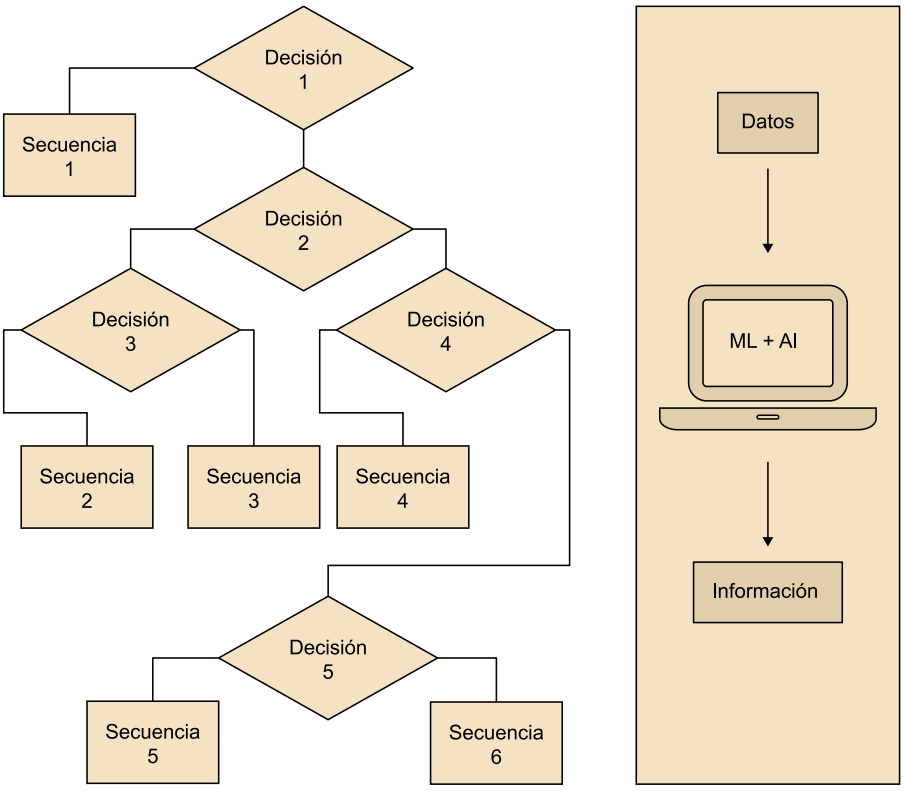
En este contexto es donde el diagrama de Venn de Drew Conway, que tenemos en la figura 15, nos es de ayuda. Es una representación muy sencilla que representa las competencias (digamos mínimas) en el ámbito de la seguridad gestionada a partir de la analítica de datos. Para Drew, se necesita combinar la estadística con el análisis de datos, técnicas de visualización y disponer de la adecuada potencia de cálculo en nuestros sistemas y los correctos conocimientos de seguridad. Pero, si queremos trabajar aquí, hemos de disponer de dos habilidades que son vitales: la curiosidad y la comunicación, y aquí es donde lo que denomina las competencias de *hacking* juegan un papel vital: hemos de ser unos verdaderos apasionados de la tecnología para llevarla a nuestros intereses, hemos de ser capaces de transformar la realidad y de adaptar nuestro entorno para llegar al objetivo último del control del sistema y sus procesos.

Hemos de tener una alta dosis de criticidad y hemos de cuestionarlo casi todo, para poder llegar a descubrir, en los más recónditos rincones de los procesos y sistemas, la verdadera realidad de la (in)seguridad.

No es imprescindible aunque lo indique un gran experto en estadística y matemática; lo que sí es importante es que en el equipo haya dicho perfil, y que tenga una buena capacidad de comunicación, acompañada por nuestra capacidad de entender los conceptos y fundamentos de dicha ciencia, para poder caminar hacia nuestro objetivo.

Una buena fuente de datos, para empezar a caminar por esta senda, puede ser la base de datos de AlienVault (13), y hacer una lectura al breve pero intenso libro de Raffael Marty (14).

Figura 16. Sistemas basados en reglas frente a los basados en la analítica de datos



La realidad es que cada vez es más frecuente trabajar la ciberseguridad desde el prisma de la analítica de datos. Cada vez disponemos de más datos, y nuestra capacidad de extraer información de ellos está cada vez más desarrollada. Por ejemplo, en los sistemas de detección y prevención de intrusiones, cada vez son más recurrentes estas técnicas que superan en prestaciones a las basadas en reglas (ver figura 16), pues requieren en el fondo menos recursos (sobre todo humanos), y acaban siendo más dinámicas, adaptativas. Podríamos pues decir que los factores que están impulsando la adopción de soluciones basadas en analítica de datos, inteligencia artificial o *machine learning* son:

- Velocidad (de proceso y tratamiento de los datos en busca de vulnerabilidades, frente a las soluciones secuenciales basadas en reglas).

- Escalabilidad (pueden adaptarse, fácilmente, cuando la cantidad de información a manejar aumenta, por ejemplo, por un aumento considerable del tráfico en nuestros equipos de detección de intrusiones).

- Automatización (de los procesos de readaptación).

- Adaptabilidad (muy importante para hacer frente a las soluciones de ataque que son cada vez más de día cero).

- Personalización (en su capacidad de adaptarse, nuestras soluciones de seguridad serán las adecuadas para nuestro entorno y no serán una réplica de las impuestas en otras organizaciones, con retoques menores).

En el ámbito de la gestión de *malware* cada vez es más recurrente utilizar estas soluciones (15). Las soluciones basadas en firmas no son adecuadas para hacer frente a ataques de día cero, y tampoco nos van a poder detectar aquellas amenazas de tipo metamórfico o polimórfico, lo que nos llevaría a elevadas tasas de falsos positivos en las aproximaciones basadas en la detección de anomalías[88].

(88)Un elevado número de falsos positivos, si bien nos puede dar una sensación de seguridad, nos va a ralentizar todos nuestros procesos. La seguridad no debe ir en contra de las actividades fundamentales del negocio, sino que debe siempre estar alineada con el negocio. Si nuestros controles lo paran todo, no estamos desplegando buenas políticas de seguridad, estamos disminuyendo y afectando en alta medida nuestra capacidad productiva.

Las soluciones automatizadas van a permitirnos (después de analizar grandes cantidades de datos) encontrar patrones que sí vamos a poder utilizar, pues son los que acabarán siendo recurrentes en las alternativas de ataque. El elemento diferenciador es la automatización, la adaptación y el tratamiento de enormes cantidades de datos para la identificación de los patrones. Pero quizás el factor más importante de las soluciones analíticas es su capacidad predictiva. Podemos en cierta forma adelantarnos al futuro, y por lo tanto seremos capaces de detectar variantes de ataques actuales. Igual que el ataque adapta los mecanismos de ataque, nuestros algoritmos predictivos van a poder estimar cuáles serán los patrones de vulnerabilidades del futuro (16). Y este sí es un factor ganador y diferenciador, que nos debe llevar hacia el uso de las técnicas analíticas en los algoritmos y soluciones de ciberseguridad que vayamos a implementar (17).

Es un procedimiento de aprendizaje de dos fases[89]:

(89)En inglés se utiliza el término *two-level learning approach*.

- Fase de aprendizaje supervisado (18), donde vamos a detectar los flujos maliciosos e identificarlos (tipificarlos). Pero, con este modelo supervisado, no vamos a poder hacer frente a los nuevos vectores maliciosos.

- Fase de aprendizaje no supervisado, donde vamos a hacer frente a todo lo que es nuevo.

Una buena manera de empezar es con el paquete `adversarialib` (19), un conjunto de herramientas *open source* para evaluar nuestras soluciones de *machine learning*.

De hecho, tal y como nos indicaba en 2016 Ram Shankar (20), la seguridad derivará en un servicio en Cloud, marcado por tres factores claros:

- El servicio permitirá la gestión de todos los datos de monitorización que se deben considerar.

- Los costes distribuidos en una solución Cloud permiten mejores soluciones para cada uno de los clientes que las que ellos van a poder autoproveerse.

- La rápida evolución de las herramientas de seguridad solo va a ser posible a muy gran escala. Si no pertenecemos a este reducido grupo de organizaciones, la única oportunidad que tenemos es la de agruparnos, y la mejor manera de hacerlo es a través de un proveedor de servicios de seguridad (en Cloud).

1.2.5. Ciberseguridad en entornos IoT

Como es bien conocida la evolución que hemos tenido en internet, no vamos a ahondar mucho aquí en ello, pero sí vamos a recordar que hemos pasado, en unos veinte años, de la era de los contenidos a la de los servicios; de la era de los proveedores a la de las personas y cosas. Todos estamos ahora continuamente conectados, pero ello, para los responsables de seguridad, nos supone una carga más de problemas, pues son nuevas fuentes de ataques en nuestro entorno.

En un entorno hiperconectado, todos estos dispositivos, que tienen, en algunos casos información nuestra altamente sensible (tanto de salud como de nuestro hogar o de nuestras cuentas bancarias), van a ser vectores de ataque mucho más accesibles que nuestros servidores, nuestros ordenadores de sobremesa o nuestros terminales móviles.

Se habla de más de cincuenta billones de dispositivos antes del año 2030, y esto nos obliga a escuchar cómo nos va a afectar desde la perspectiva de la seguridad.

Existen ya muchos (demasiados) casos de vulnerabilidades en entornos IoT. Por ejemplo, recordemos el caso derivado de vulnerabilidades en cámaras wifi, donde se expusieron dispositivos vulnerables al ataque de *botnet* Mirai, que

permitía, por un lado, el rápido descubrimiento de la cámara y, por otro, el acceso al dispositivo por una falta de políticas de acceso adecuadas. Por ejemplo, el informe de 2014 (21) ya revelaba que más del 70 % de los dispositivos que podríamos englobar en el mundo del IoT tenían muy importantes vulnerabilidades. En este informe se analizaron diversos fabricantes de televisores, webcams, termostatos domésticos, enchufes controlables remotamente, aspersores controlables remotamente, *hubs* para la interconexión de múltiples dispositivos en entornos domésticos, cerraduras, alarmas domésticas, sistemas de abertura de garajes... Lo primero destacable del informe es que, ya entonces, la mayoría de los dispositivos disponían de algún servicio en Cloud, con aplicaciones móviles para su control remoto. Lo terrible del informe es que se llegaron a encontrar un promedio de veinticinco vulnerabilidades (serias) por tipo de dispositivo, destacando:

- Aspectos relativos a la privacidad: un 90 % de los dispositivos disponían, en la aplicación móvil o el servicio en Cloud, de datos privados que no se trataban de la forma adecuada.

- Aspectos relativos a mecanismos de autenticación: un 80 % de los dispositivos tenían graves insuficiencias con su política de contraseñas (en cuanto a robustez, longitud y caducidad).

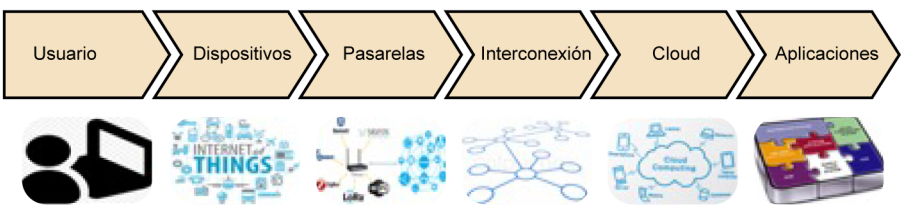
- Aspectos relativos al cifrado: un 70 % de los dispositivos no tenían ningún mecanismo de encriptación de sus comunicaciones en internet, ni por supuesto sus comunicaciones locales, lo que permite (permitía) la muy fácil captura de información por parte de potenciales atacantes.

- Aspectos relativos a la seguridad de sus interfaces web: en un 60 % de los casos, estas eran vulnerables a ataques típicos de persistencia o problemas con las credenciales.

- Aspectos relativos a los procesos de actualización de software: en un 60 % de los casos, las descargas de actualizaciones se hacían sin ninguna medida de cifrado ni de firma de lo descargado.

La gestión de la seguridad, en el caso de los entornos IoT, abarca toda la cadena, desde el usuario a aplicaciones de terceros (muchas veces en Cloud), como podemos ver en la figura 17.

Figura 17. Gestión de la seguridad en entornos IoT. Un enfoque transversal



Aunque nos parezca que IoT es un problema básicamente doméstico, nada más lejos de la realidad, ya que los sistemas de control industrial (sea en forma de ICS[90] o de SCADA[91]) todos tienen la misma problemática, y la criticidad de su vulnerabilidad es mucho más alta[92].

(90)En inglés se utiliza el término *industrial control system* (ICS).

(91)En inglés se utiliza el término *supervisory control and data acquisition* (SCADA).

(92)Un buen ejemplo es el ataque a una planta de producción energética en Ucrania.

De todas formas, el ecosistema del mundo IoT es mucho más que la seguridad de los dispositivos. Es un aspecto de múltiples dimensiones y que nos obligará a tratar de forma absolutamente global y transversal. De hecho, no hacemos más que recopilar todas y cada una de las posibles fuentes de vulnerabilidad (comunicaciones, aplicaciones, interfaces de usuario, sistemas operativos y *firmware*) en un nuevo entorno, que además debe ser eficiente en su funcionamiento, y esta es su gran debilidad (22). Al tener que diseñar soluciones que sean eficientes en aspectos relacionados con el consumo, la eficiencia de las comunicaciones y la memoria disponible, se peca de olvidar aspectos fundamentales de la seguridad que suponen un gran riesgo.

Un buen punto de partida es mirar las diez recomendaciones OWASP[93] (23) sobre IoT, que divide los diferentes ámbitos a analizar y securizar para minimizar los riesgos en implementaciones en entornos IoT (24):

(93)OWASP - Open Web Application Security Project es una organización sin ánimo de lucro focalizada en la securización de aplicaciones.

- Control de acceso, incluyendo elementos de autenticación, gestión de sesiones, relaciones de confianza (a veces demasiado automáticas) entre las partes, componentes de registro, procedimientos de pérdida de credenciales.

- Gestión de memoria, incluyendo sobre todo elementos de almacenamiento de información en las aplicaciones y los dispositivos, como pueden ser nombres de usuario (y obviamente contraseñas) en claro, las credenciales de terceros, o las propias claves de encriptación.

- Gestión del *firmware* del dispositivo, incluyendo por ejemplo las contraseñas incrustadas en el *firmware*[94], conceptos de direcciones que no deberían poder conocerse[95], y lo mismo con algunas claves de encriptación.

(94)En inglés se utiliza el término *hardcoded*.

(95)En inglés se utiliza el término *URL disclosure*.

- Interfaces web, para proteger de ataques en aplicaciones web, como podrían ser las inyecciones SQL, los ataques CSS[96], los ataques por enumeración de nombres de usuarios, las contraseñas débiles…

(96)En inglés se utiliza el término *cross-site scripting*.

- Servicios de red de los dispositivos, que pueden permitir el acceso a información confidencial y relevante a través de defectos de configuración para el acceso a las interfaces de comandos de los dispositivos, sobre todo sin controlar adecuadamente la elevación de privilegios, y a nivel de ataques de denegación de servicios, de los servicios en red de los dispositivos (25).

- Mecanismos de almacenamiento locales, que no gestionan de forma adecuada la encriptación y cifrado de la información, o que cifra la informa-

ción con unas claves que no están adecuadamente securizadas, o la gestión deficiente de la integridad de los datos almacenados.

- Gestión de las API de terceros, que en muchas ocasiones nos hace trabajar con soluciones que no protegen con el nivel necesario la privacidad de ciertas informaciones personales, o que establecen comunicaciones con pocos niveles de garantía, y deficientes procedimientos de control de acceso y autenticación. Es importante disponer de API para la gestión y programación de funcionalidades y servicios sobre los dispositivos de terceros, pero debemos conocer la gestión de la seguridad que dichos fabricantes tienen implementada, y, sobre todo, cómo se aplica en las API que nos proporcionan.

- Mecanismos de actualización, donde es importante los procedimientos de autenticación e integridad de las actualizaciones que se vayan a descargar y actualizar en los dispositivos. Hemos de validar de dónde viene la actualización y su integridad, y el canal a través del cual se ha producido la actualización también.

- Tráfico en nuestra red local, y nuestras conexiones con el exterior, para poder monitorizar y controlar flujos incorrectos.

Seguramente, como siempre, la mejor manera de hacer frente a la seguridad global de nuestro ecosistema IoT es a través de un análisis por capas[97]:

(97)En este sentido, es interesante mirar el estudio «Understanding IoT Security», de IOT Analytics, en colaboración con George Cora, CEO de Ardexa, una compañía de seguridad en el ecosistema IoT (223).

1) Seguridad en el dispositivo (de terminal[98]): estamos en la capa hardware de nuestra solución IoT. En este aspecto, es fundamental que en ODM y OEM (la parte de diseño y producción de los dispositivos) cada vez se integren más medidas de seguridad, tanto en el hardware como en el *firmware*. Podríamos enumerar aspectos relativos a seguridad a nivel de chip (en aspectos, por ejemplo, relativos a perfiles de *root*), o aspectos relativos a modos de arranque (que, por ejemplo, solo lo hagan en caso de haber certificado y validado el software con el que se va a arrancar el dispositivo), o aspectos de seguridad física del dispositivo (para evitar que un intruso pueda tener acceso físico al dispositivo a través de manipulación del mismo).

(98)En inglés se utiliza mucho el término *endpoint security*.

2) Seguridad a nivel de comunicación (de conectividad). En el momento que transmitimos información desde el dispositivo hacia otros elementos de nuestro sistema, la forma de enviar los datos y los mecanismos de protección implementados son de gran importancia para la seguridad del entorno en global. Es importante, en este aspecto, incrementar la capacidad de proceso y tratamiento de datos en forma local en los dispositivos[99]. Uno de los principales puntos de vulnerabilidad vendría en forma de ataques del tipo *man-in-the-middle*, y la forma de evitarlos pasa por una alta securización de los canales de comunicación, la utilización de dispositivos de seguridad perimetral (en forma de cortafuegos, o sistemas de detección y prevención de intrusiones)

(99)En inglés se utiliza mucho el término *edge processing*.

que vamos a utilizar para una monitorización constante de las comunicaciones con nuestros dispositivos IoT, para el análisis de todos los flujos de comunicaciones, para poder detectar posibles intrusiones que luego puedan derivar en males mayores. En el ámbito de las comunicaciones, una de las principales recomendaciones es el punto de inicio de la comunicación. Si las comunicaciones con el mundo exterior siempre las inicia el propio dispositivo, es más complicado que se puedan producir comunicaciones con terceros dispositivos no permitidos.

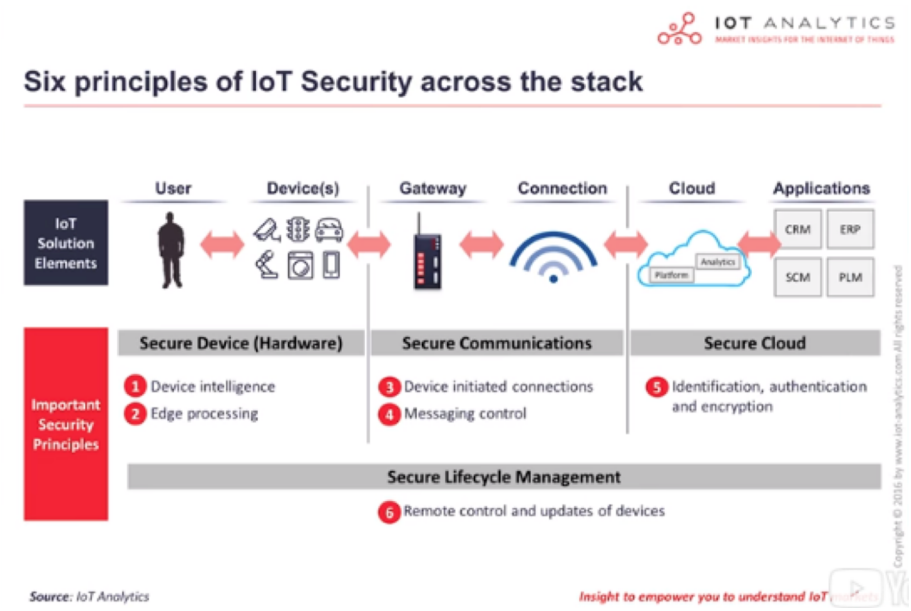
En este sentido, hay que andar con mucho cuidado con las soluciones a medias. Por ejemplo, en algunos casos se implementan sistemas cerrados de comunicación (que no pasan por internet[100]), pensando que así ya mantenemos un alto nivel de seguridad, pues cerramos uno de los vectores de infección. Pero puede vulnerarse la seguridad del dispositivo en la primera de las capas (por ejemplo, a nivel de *firmware* en una actualización no controlada), y nuestro sistema cerrado de comunicación ya no es una garantía de nada.

(100)En inglés se utiliza mucho el término *out of band* (OOB).

3) Seguridad en Cloud. En este caso, el punto relevante es la infraestructura (sobre todo software) que constituirá el *back-end* de nuestra solución IoT. Es el punto de concentración de todos los datos que vayamos a recopilar, para luego analizarlos, interpretarlos y generar acciones. Por un lado, tenemos aspectos relativos a la gestión de la privacidad de la información almacenada en Cloud (que puede incluir muy fácilmente datos de alta sensibilidad), que debe ser protegida mediante mecanismos de cifrado. Las plataformas de gestión de identidades son cruciales en este aspecto.

4) Seguridad en la gestión del ciclo de vida de todo el proceso, que nos va a garantizar que los niveles de seguridad con los que estamos trabajando perduran a lo largo del tiempo, incluso con la entrada de nuevos vectores de infección. Este proceso pasa por garantizar que los controles que se están implementando son los adecuados en forma, número y periodicidad de actuación.

Figura 18. Seis principios básicos de seguridad en entornos IoT según IOT Analytics (26)



Desde IOT Analytics (como vemos en la figura 18) se resumirían los seis principios básicos a tener en cuenta para incrementar nuestro nivel de seguridad en:

- Ampliar la capacidad de análisis (inteligencia) en los dispositivos, para por ejemplo validar las actualizaciones de *firmware*.

- Ampliar la capacidad de procesamiento en los dispositivos, para mejorar por ejemplo la seguridad de las comunicaciones.

- Establecer solo comunicaciones iniciadas desde el lado dispositivo, para evitar el establecimiento de comunicaciones con interlocutores no autorizados.

- Aumentar el nivel de control sobre la mensajería de nuestras comunicaciones (en los protocolos de comunicación).

- Aumentar el nivel de seguridad en la capa de gestión de identidades para una mejor autenticación de los interlocutores de las comunicaciones, y en los procedimientos de firma y cifrado, para una mejor protección de las comunicaciones entre interlocutores autorizados.

- Mejorar el ciclo de gestión de la seguridad de forma continuada, con especial énfasis en la parte de actualizaciones de los dispositivos, y en la parte de las conexiones remotas habilitadas hacia los dispositivos.

1.2.6. Protección de infraestructuras críticas

En España, debemos seguir la Ley de protección de infraestructuras críticas (PIC), que se deriva de la Directiva Europea de NIS (Network and Information European Directive). Directiva europea vigente desde mayo de 2018.

El referente es la NIS, que luego se concreta en leyes estatales específicas. En el caso de España, la PIC protege al ciudadano de ataques a infraestructuras que pueden dañar o perjudicar a ciudadanos: trenes, centrales nucleares, eléctricas, gas, aeropuertos, etc. Con la PIC se protege al ciudadano de problemas en servicios esenciales (*utilities*, sanidad, transporte…) y servicios de internet (Google, Instagram…).

Los aspectos más detallados referentes a la protección de infraestructuras críticas los veremos en el capítulo 5.

1.2.7. Evaluación de activos y riesgos en entornos industriales

Cuando vamos a poner en marcha un procedimiento de gestión del riesgo, lo primero es saber a partir de qué, para qué… Las razones pueden ser muy diversas: pueden ser de índole meramente relacionadas con el negocio (alguna actividad, digamos, meramente mercantil), o pueden tener relación con una actuación tecnológica (por ejemplo, poner en marcha una nueva base de datos para algún propósito específico).

Este primer aspecto nos va a definir el objetivo y el ámbito del programa de gestión del riesgo que vamos a implantar, y además, nos va a identificar quién es el promotor de la actuación (esta figura es muy relevante).

Si conocemos el promotor, podremos definir de forma clara cuál es el objetivo de la actuación, y podremos dar respuesta en este momento (y con el promotor) a todas las preguntas relacionadas con esta definición. Seguidamente, debemos identificar todos los activos que estarán asociados con la actuación. Es el momento de clasificar el impacto en el negocio que podemos padecer: impacto alto, impacto moderado, impacto bajo[101].

[101]En inglés se suele utilizar los términos *high business impact* (HBI), *moderate business impact* (MBI); *low business impact* (LBI).

Es importante organizar de forma adecuada al equipo que va a trabajar en la gestión del riesgo; cuanto más diverso, con el grado de responsabilidad adecuado, mejor. Sería conveniente (en un entorno de gestión de la seguridad) disponer de los siguientes cuatro perfiles:

- Alguna persona con un alto nivel de responsabilidad de gestión en la compañía. Será el enlace con el negocio, quien tenga capacidad de decisión en cuanto al presupuesto. Ha de ser una persona con capacidad de decisión.

- Alguna persona del ámbito de la seguridad (si disponemos de la figura del CISO sería el perfil más adecuado). Es el perfil que va a tener la responsabi-

lidad de cuantificar (o explicar) las probabilidades, los riesgos, el impacto con el negocio y los activos.

- Alguna persona responsable (propietaria) de los sistemas o de la información afectada. Un perfil adecuado sería alguien del ámbito del desarrollo de negocio. Debe conocer muy bien el negocio con el que tiene relación la actuación que vamos a desarrollar. Con su responsabilidad asociada al negocio, ha de tener la capacidad de tomar decisiones y evaluaciones en términos de coste-beneficio (de las acciones a implantar).

- Alguna persona del ámbito de las operaciones (alguien de IT, ingeniería, producción…) con conocimientos, y responsabilidades tecnológicas y capacidad de gestión y organización de los recursos asociados, con capacidad para determinar los costes de las operaciones asociadas.

Para una información más detallada de los aspectos relativos a la gestión de la ciberseguridad en entornos industriales, nos podemos referenciar a los capítulos 3, 4 y 5.

1.2.8. Procedimientos estandarizados

En el ciclo continuado de gestión de la ciberseguridad podemos seguir los ejemplos de otros sectores que han definido diferentes metodologías para afrontar las diferentes situaciones de riesgo.

De forma genérica, se definen:

- Planes de implementación, a veces referidos como guías de implementación (o de configuración) que van a dar las pautas para la correcta puesta en marcha de las diferentes soluciones, aplicaciones, sistemas y procesos que permitan asegurar el nivel de garantía demandado por las normativas o los propios procedimientos de la organización. El despliegue de las soluciones debe hacerse de forma metódica siguiendo pautas claramente documentadas, testeadas y validadas, que no pueden permitir en ningún caso la improvisación por parte del personal que lleva a cabo la implantación.

- Planes de mejora continuada, que permiten conocer los mecanismos, indicadores y elementos para la certificación de que las soluciones implantadas funcionan de la forma esperada en el diseño y guías de implementación, y que no han aparecido hechos o situaciones que puedan provocar un incidente de seguridad no controlado.

- Planes de gestión del riesgo, que deben tener en consideración la forma de actuación ante un incidente de seguridad. La gestión de los incidentes no puede dejarse al azar del personal que esté en cada momento *in situ*, sino que debe analizarse con previsión temporal, intentando tener en consideración todas las situaciones y casuística con la que nos podamos encontrar

en un caso real. Para cada una de las situaciones, deberán ponerse sobre la mesa los protocolos de respuesta.

Analicemos, en este sentido, un par de documentos que nos pueden dar una idea aplicada al entorno de la gestión de la ciberseguridad, si bien en los dos siguientes capítulos detallaremos mucho más dos de las normas más relevantes en este aspecto en el sector de la ciberseguridad.

CSIP (*cybersecurity strategy and implementation plan*)

Un plan estratégico de seguridad nos dará una pauta de las prácticas de seguridad de la organización, así como de cuáles van a ser los objetivos a atacar a corto plazo (por debajo de los doce meses), a medio plazo (entre dieciocho y veinticuatro meses) y a largo plazo (para los próximos treinta y seis meses). La gestión del documento (del plan) debe estar dirigida por el CISO (si la figura existe en la organización), y debe ser un documento vivo, de forma que los objetivos (como mínimo) deberán revisarse anualmente por parte de algún órgano creado en la organización para este propósito (algún comité ejecutivo con responsabilidades en ciberseguridad).

Para la definición del plan, primero deberemos tener una clara y concreta foto del punto en el que los aspectos de seguridad están en la organización. Si estamos desplegando el primero de los planes, deberemos hacer un análisis muy minucioso de estos aspectos; si, por el contrario, se trata de una revisión de un plan anterior, deberemos revisar la información de la que disponíamos en el documento de partida, y poder validar que no tenemos nuevos condicionantes a tener enmarcados en el documento. Evidentemente, como ya se ha indicado antes, deberemos revisar de forma continuada cuáles son los activos (importantes) de la organización (en los que vamos a focalizar los mayores esfuerzos de seguridad). Para cada uno de estos activos, como hemos indicado, tendremos que hacer una identificación de amenazas, vulnerabilidades, riesgos y estimación del impacto (en caso de incidente de seguridad) para poder priorizar las contramedidas de seguridad que podamos marcar en nuestra planificación estratégica.

A continuación, utilizando (por ejemplo) alguna de las metodologías estandarizadas (ISO, COBIT, NIST que podamos ver a continuación), se va a establecer un punto de partida de la seguridad corporativa. Este elemento es crucial para, en el futuro, poder valorar las mejoras conseguidas en nuestra política de seguridad, o para marcar unos claros objetivos en dicho aspecto a conseguir a corto, medio o largo plazo.

En la definición de la visión del plan estratégico se suele incorporar alguna frase del tipo: «incorporar una actitud proactiva de seguridad en todos los procesos de negocio de la organización», que permita indicar que la ciberseguridad es un elemento que se va a tener en cuenta en todas las decisiones de negocio.

Un aspecto que no debe nunca obviarse del plan estratégico de seguridad es su gobernanza. ¿En qué nivel de decisión de la organización tenemos situada la gestión del plan? Es importante conseguir que el plan (como estratégico que es) sea aprobado por el órgano de decisión de la organización de mayor nivel posible, para que tenga un verdadero respaldo por parte de la organización. Por ejemplo, debería aprobarse anualmente en los máximos órganos de decisión de la organización.

Los objetivos estratégicos del plan estratégico de seguridad deben tener en consideración aquellos casos de ciberseguridad que se hayan tenido en la organización (o de los que tengamos conocimiento en otras organizaciones de nuestro mismo sector), para garantizar que damos respuesta a situaciones reales de riesgo. Por ejemplo (27), podemos estructurar algunos de los objetivos:

- Objetivo de seguridad: prevenir la pérdida de datos.

- Elementos que justifican el objetivo: las políticas de seguridad, los estándares (deberíamos enumerar cuáles), las guías de buenas prácticas…, los informes de auditorías de seguridad que hacían referencia a algún riesgo de este ámbito.

- Resultados esperados (generalistas): prevención de la pérdida de información (datos), mejorar los niveles de seguridad de los sistemas y servicios de red corporativos, disponer de elementos de gestión de la seguridad de la información proactivos, garantizar la mejora continuada de los mecanismos de gobernanza corporativa.

- Descripción: desarrollar, aprobar y poner en marcha un conjunto de políticas de seguridad de la información, siguiendo las recomendaciones al respecto de la protección de datos de la ISO/IEC 27001.

- Resultados de aplicación: que deben tener siempre un alineamiento con el negocio:
  - Definición de los procesos referentes a la política de protección de datos, para todos los departamentos de la organización.

  - Definición de los procesos de métrica para garantizar la adecuada implantación de las medidas, y de su eficiencia, en todos los procesos de la organización.

- Requerimientos: listado de los servicios, aplicaciones, sistemas necesarios para el despliegue de las soluciones. Deben también tenerse en consideración los equipos humanos y las consideraciones de tiempo (horas del equipo) para una correcta evaluación realista de los esfuerzos necesarios.

Aunque cada documento es particular, y diferente de los de otros sectores u organizaciones, siempre es bueno poder referenciar algunos ejemplos como pauta de inicio de nuestro documento estratégico. A tal efecto, se puede mirar el documento estratégico a escala nacional de la República de Eslovaquia (28).

Otro ejemplo podría ser el documento del Gobierno Federal de Estados Unidos (29), donde se exponen cinco objetivos estratégicos:

- Identificación (prioritaria) y protección de los activos e información de alto valor estratégico.

- Detección (a tiempo) y despliegue de los mecanismos de respuesta rápida adecuados para dar respuesta a futuros (posibles/probables) incidentes de ciberseguridad.

- Definición de procesos para la rápida garantía de la continuidad de las actividades afectadas por posibles incidentes de ciberseguridad, y la puesta en marcha de los procesos que permitan garantizar la mejora continua de los mecanismos de protección, sobre la base de todo lo aprendido de anteriores situaciones de riesgo o incidentes reales de seguridad.

- Definición de los procesos de contratación y retención de los equipos humanos necesarios para hacer frente a las situaciones de ciberseguridad (nacional).

- Concreción de los procesos de adquisición (eficiente y efectiva), así como de su posterior puesta en marcha de las (mejores) soluciones tecnológicas (existentes o futuras).

CSCRM (*cyber supply chain risk management*)

Este plan responde a la necesidad de identificar, evaluar y posteriormente mitigar los riesgos asociados con la naturaleza distribuida (e interconectada) de la cadena de fabricación (desde la perspectiva IT y OT). Debe, pues, cubrir el ciclo de vida completo de los sistemas, desde su diseño, desarrollo, distribución, puesta en marcha, mantenimiento y finalmente parada y (eliminación), y en todo este proceso deben tenerse los procesos y medidas adecuados para la gestión de la ciberseguridad, en aspectos tales como amenazas, vulnerabilidades, riesgos, contramedidas y gestión de los propios incidentes de seguridad.

En la recomendación de NIST (30) se afrontan los siguientes aspectos fundamentales:

- Buenas prácticas de base: dado que CSCRM está entre dos mundos, el de la cadena de fabricación (muy OT) y el de la ciberseguridad (muy IT), deben

conjuntarse las buenas prácticas de los dos mundos para una adecuada gestión global del problema.

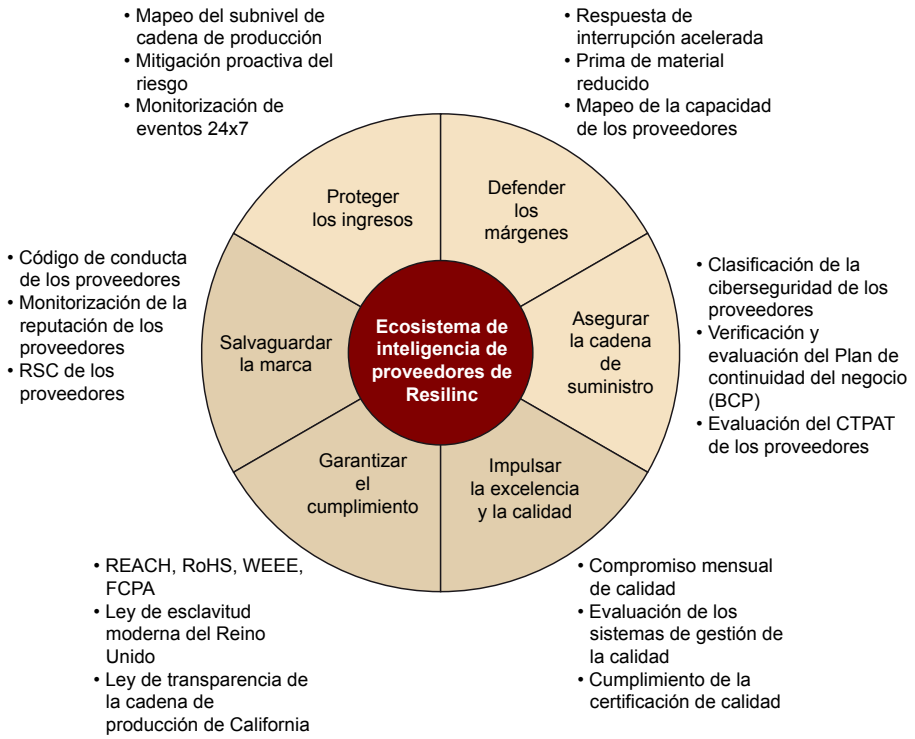
- Implicación total de la organización: este es un asunto absolutamente transversal de la organización y, por lo tanto, en su gestión deben tenerse en consideración todos los estamentos de la organización: desde los aspectos estratégicos de la misión, los procesos de negocio, los sistemas de información, pero también deben considerarse todas las unidades de la organización, como pueden ser la de ciberseguridad, la de producción y fabricación, la de compras, jurídico-fiscal, ingeniería… y, por supuesto, su despliegue debe considerar todo el ciclo de vida de los productos de la organización. Es un plan de alta complejidad (empezando desde el aspecto organizativo y de gestión).

- La gestión del riesgo. Los aspectos de la gestión del riesgo de la ciberseguridad en la cadena de fabricación no pueden considerarse como aislados del resto de procesos que tienen mecanismos de gestión del riesgo en la organización. Como todos ellos, deben seguir las pautas habituales definidas al principio de este capítulo para la gestión de la ciberseguridad, pero cuando las acerquemos a nuestro caso práctico particular, debemos entender que cada situación, de cada organización y de cada momento, va a requerir unos mecanismos de gestión del riesgo particulares.

- La gestión de los sistemas críticos, propios de toda cadena de fabricación, que deban tener una consideración especial respecto a sus medidas de control y seguridad, por el importante impacto que un ataque o incidente de seguridad sobre ellos pueda tener en el negocio de la organización.

En la figura 19 podemos ver un ejemplo de solución de gestión de riesgos en la cadena de fabricación basado en la solución de Resilinc Corporation (31), (212) y (231).

Figura 19. Gestión integral de riesgos en la cadena de fabricación



1.3. Estándares de ciberseguridad

Vamos a enumerar, brevemente, algunas de las plataformas y estándares que tienen relación con la gestión de la seguridad y la gestión de riesgos en entornos IT.

Los estándares y plataformas son muy importantes para, por un lado, tener los procedimientos y mecanismos para gestionar la seguridad, pero por otro lado para tener una lista (conocimiento) de las prácticas, guías y protocolos que debemos aplicar en cada momento.

Algunas de las soluciones pueden ser COBIT[102] (de ISACA[103]), ISO 27001 o/y ISO 27002. Nos ayudarán con recomendaciones y metodologías, y nos aconsejarán en qué momento debemos aplicar la gestión del riesgo y de qué forma en nuestras organizaciones. Por lo general, las aproximaciones de las diferentes plataformas o estándares son similares, aunque cada una tiene sus propios objetivos (a alto nivel). Por ejemplo, OCTAVE, NIST o ISO 27005 se focalizan en la gestión de la seguridad, mientras que específicamente para la gestión del riesgo es mejor utilizar COBIT, ISACA (muy enfocada para disponer de guías prácticas, comparativas[104], y la gobernanza IT, para prácticamente cualquier tipo de compañía y negocio, que hagan uso de sistemas de información (32).

El número y ámbito de las recomendaciones y estándares que podemos encontrar es enorme. Una buena fuente de recopilación (33) los estructura de la siguiente forma:

[102]COBIT: *control objectives for information and related technology*.

[103]Information Systems Audit and Control Association

[104]En inglés *benchmarks*.

- Guías y políticas de seguridad.
- Estándares.
- Guías para la gestión de negocios y actividades en línea.
- Guías para la gestión de la privacidad.
- Otras referencias.

A continuación, hacemos referencia a algunos de ellos. Utilicemos la recomendación que utilicemos, en todo momento es conveniente seguir algunas recomendaciones básicas del National Institute for Standards and Technology, que enumeramos (34):

- Debemos enfocarnos a nuestros riesgos, de dónde proceden, cómo podemos prevenirlos o reducirlos. Debemos ser capaces de generar y luego utilizar métricas adecuadas.
- Debemos ser capaces de modelar y evaluar un amplio margen de modelos de predicción de fallos.
- Debemos ser capaces de sistematizar la analítica de nuestro sistema, para que además de ser repetible en sus medidas, sea auditable y verificable.
- Debemos alinear los procedimientos y herramientas a utilizar con las habilidades y competencias de las personas que las van a poner en práctica. Debemos garantizar, además, que las cargas asociadas no van a ser excesivas.
- Debemos estar seguros de que el nivel de complejidad en la operación es el adecuado para nuestro entorno y nuestro contexto.
- Debemos estar seguros de que la información que obtengamos es interpretable (recordad siempre que las representaciones gráficas ayudan mucho).
- Debemos garantizar que la información extraída sea adecuada, en cantidad y calidad.
- Debemos garantizar que podemos integrar los resultados y el proceso completo en alguno de los procesos del ciclo de vida de nuestro sistema de gestión de la seguridad.
- Debemos garantizar la integridad de las herramientas y soluciones utilizadas, en el sentido de que debemos garantizar continuidad de las mismas.

- Debemos tener el soporte de alguna organización de estandarización, sea nacional o internacional, o documentos de referencia, para poder sustentar de forma adecuada nuestro proceso y nuestras conclusiones.

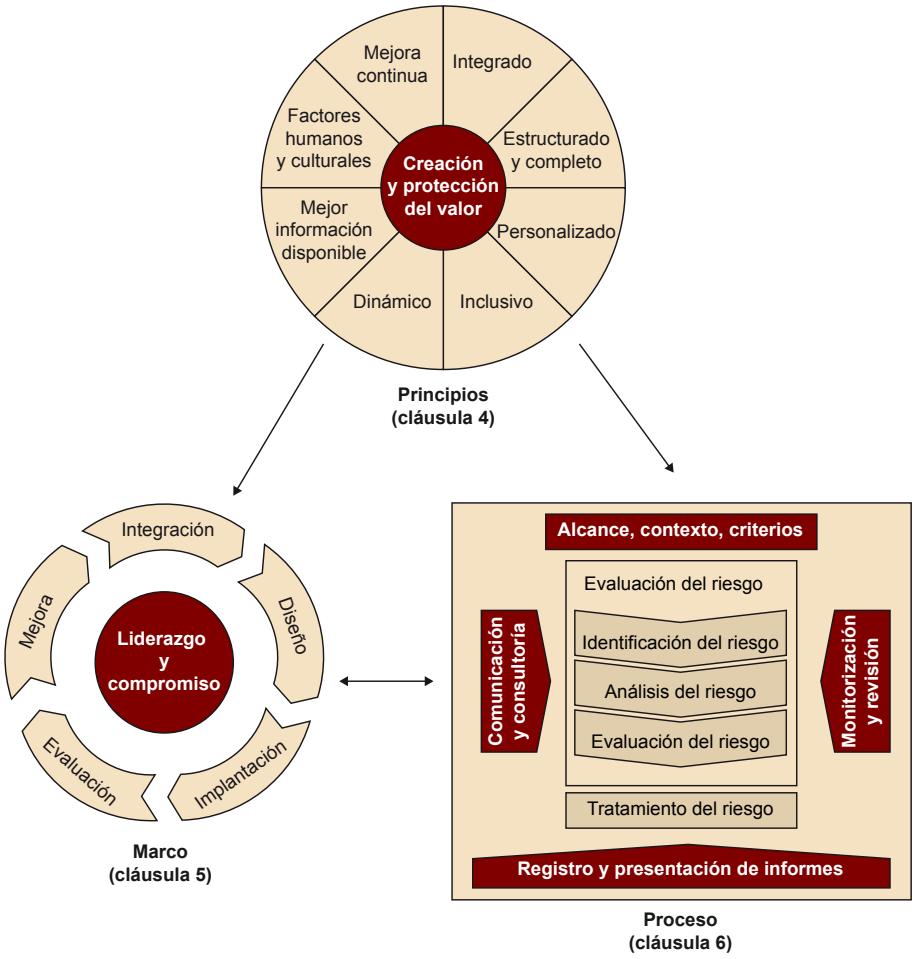
- Debemos estar seguros de que las herramientas y procesos a implantar estarán alineados con nuestra cultura organizativa.

1.3.1. ISO/IEC 31000:2018

Conjunto de estándares (35) para el análisis de riesgos, considerando la toma de decisiones en un contexto de riesgo, adaptando los modelos de gobernanza y todos los procesos que de la gestión del riesgo se puedan derivar, en aspectos de planificación, gestión, comunicación, definición de políticas, gestión de valores y activos de la organización o incluso en aspectos culturales.

Es un sistema abierto, basado en un conjunto de principios que vamos a poder adaptar a la idiosincrasia de cada organización, pues es aplicable para cualquier tipo, tamaño, sector de actividad o ubicación, y en cierta forma cubre todo tipo de riesgos.

Figura 20. Principios, plataformas y procesos de IEC/ISO 31000



1.3.2. ISO/IEC 22301

Normativa (36) para el sistema de gestión de continuidad de negocio[105], que toma como referencia la normativa británica BS25999 (37), que podría ser utilizado por (nuevamente) organizaciones de todo tipo y tamaño. En este caso, en muchas situaciones nos encontraremos con una necesidad regulada de certificación de las organizaciones respecto a la gestión de la continuidad del negocio, sin la cual no podrán siquiera empezar a operar.

(105)En inglés se utiliza el acrónimo BCM de *business continuity management*.

Es de vital importancia, para transmitir confianza respecto a la gestión de nuestras operaciones, tanto a nuestros clientes, como a nuestra alta dirección, y como hemos dicho a las instituciones de regulación gubernamentales (nacionales y/o internacionales).

Podemos considerar sin duda el conjunto de normas asociadas con la gestión de la continuidad del negocio, desde la ISO-22301, que nos definirá una serie de requerimientos que describen los elementos básicos del sistema de gestión de la continuidad de negocio de cara al proceso de certificación y acreditación, pero también, entre otras, la ISO-22313 (38), que sería una guía de cómo desplegar las recomendaciones de la norma y que está en proceso de revisión.

1.3.3. ISACA

Actualmente, ISACA (39) representa a más de 140.000 profesionales IT, en más de 180 países, y es una plataforma para la centralización de información y guías para la auditoría de sistemas digitales (de ordenadores). Con el crecimiento tan importante que ha tenido, guarda un elevado valor por la diversidad de sus miembros, tanto por aspectos culturales o geográficos, pero también y sobre todo, por la diversidad de sectores profesionales (siempre con vinculación con la parte IT de las organizaciones) que están cubiertos desde el punto de vista de la responsabilidad en la empresa (auditoría, consultoría, seguridad IT, seguridad IS, jurídico, formación, ingeniería…) y del sector industrial de actividad de la propia organización, lo que dota de gran valor a la información que gestiona, permitiendo tener puntos de vista diversos y apropiados para el caso práctico que nos pueda ocupar en cada momento y situación.

Dispone de cuatro certificados altamente apreciados en el mercado: CISA (Certified Information Systems Auditor) (40), CISM (Certified Information Systems Auditor) (41), CRISC (Certified in Risk and Information Systems Control) (42) y CGEIT (Certified in the Governance of Enterprise IT) (43).

1.3.4. COBIT

Es una plataforma de gobernanza IT (44), con todo un conjunto asociado de herramientas, desarrolladas (avaladas o certificadas) por ISACA, para la auditoría IT. Como plataforma, la podremos utilizar para evaluar la seguridad y

poner en práctica controles sobre la información. Nos proporciona más de doscientos controles de aplicación a diferentes niveles de procesos IT o dominios de gestión.

Lo importante es que no requiere de específicos conocimientos tecnológicos, teniendo una gran orientación al proceso (al negocio). Abarca prácticamente todos los procesos IT, y tiene muy bien resuelta la conexión con el negocio y la organización (nos permitirá ver cómo tenemos relacionados nuestros procesos IT con el negocio, cómo está la parte IT alineada con el negocio, cómo nos permitirá maximizar los beneficios, cómo se potencia el negocio…); nos permitirá conocer cómo se utilizan los recursos IT de la organización (de forma responsable, adecuada, eficiente).

En general, es un entorno pensado para la dirección de la compañía, los ejecutivos, los consejos de dirección, permitiéndoles llevar a cabo de forma pertinente la gestión de la gobernanza IT, y mantener los controles y procedimientos para asegurar la seguridad de la información en la compañía.

Al enfocarse en todos los aspectos del mundo IT, y no solo la seguridad, cuando hablamos de gestión de los riesgos con COBIT, haremos referencia tanto a la seguridad como al negocio, con aspectos de desarrollo del negocio, de continuidad del negocio…

1.3.5. SERIE ISO 27000

La serie ISO 27000 se ideó específicamente para abarcar la seguridad, mientras que COBIT (por ejemplo) abarcaba todos los aspectos de IT, y la analizaremos con mucho más detalle en el capítulo 2. Es sin duda el estándar de seguridad más aceptado a escala global, incluyendo normas relacionadas con los sistemas de seguridad de la información promovidas por la Organización Internacional de Estandarización, conocida por sus siglas ISO, de International Standardization Organization.

ISO/IEC 27000 es un conjunto de estándares desarrollados –o en fase de desarrollo– por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña, estructurados de la siguiente forma (45):

- 27000. Terminología: términos y definiciones.
- 27001. SGSI certificable: requisitos de un sistema de gestión de la seguridad de la información.
- 27002 Listado de controles: objetivo de control y controles a implementar.

- 27003. Guía para implementación de un sistema de gestión de la seguridad de la información.

- 27004. Métricas e indicadores: como medida de la efectividad del sistema de gestión de la seguridad de la información.

- 27005. Análisis de riesgos, como guía de gestión del riesgo (ISO 31000).

- 27006. Proceso de acreditación de certificadores.

- Muchas otras… desarrolladas o en desarrollo.

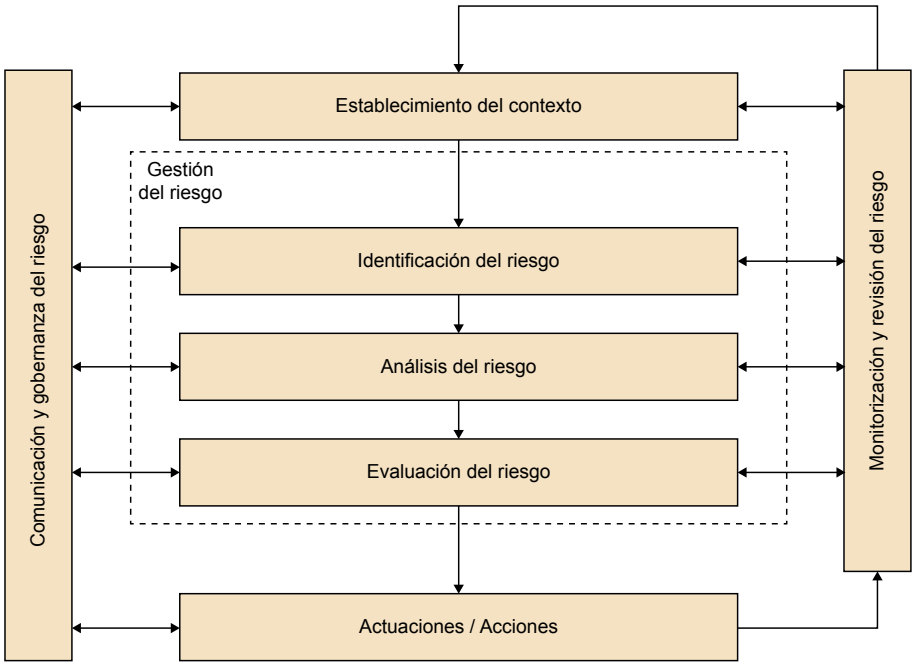
El elemento central es el sistema de gestión de la seguridad de la información (SGSI), como parte del sistema de gestión general de una organización dedicada a establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, con la finalidad última de proteger la información y los sistemas de tratamiento, frente a los riesgos de acceso, de uso, de divulgación, de interrupción o de destrucción no autorizada o imprevista, entre otros.

En su base tenemos como punto de partida NIST, siguiendo una estructura (por ejemplo, en la ISO 27005 similar), pero con un vocabulario ligeramente diferente, como podemos ver en la figura 21: hablaremos de contexto, identificación del riesgo, estimación, por un lado, y por otro, del análisis (gestión) del riesgo, donde se documentarán la probabilidad de las amenazas y los impactos asociados en el negocio.

Dispondremos de anexos, con formularios y ejemplos, que podremos o no implementar en nuestras organizaciones para evaluar y cuantificar riesgos.

Si no tenemos ninguna metodología formal para la gestión del riesgo, es un buen consejo revisar los requerimientos de gestión del riesgo de la ISO 27001 y 27002 y la aproximación global de la ISO 27005:2008.

Figura 21. Estructura de la serie ISO 27000



1.3.6. COBRA

Consultative, Objective and Bi-functional Risk Analysis es una metodología desarrollada en 1991 por C&A Systems Security, fundamentada en cuatro pilares, y con un importante enfoque sectorial bancario:

- Seguridad IT
- Riesgos operacionales
- Riesgos inmediatos o riesgos de alto nivel
- Seguridad digital

Dispone de dos herramientas básicas, una para la gestión del riesgo (46), y la segunda para la verificación del cumplimiento de ISO (47).

COBRA Risk Consultant resulta ser un servicio de análisis de riesgos muy completo, con diversas metodologías integradas para la gestión cualitativa y cuantitativa de riesgos. Es un servicio basado en cuestionarios siguiendo los principios de un sistema experto y una completa base de datos de conocimiento, que nos va a permitir evaluar las amenazas y vulnerabilidades y nos va a generar un conjunto de recomendaciones y propuestas de soluciones para ellas. Además, nos va a generar informes para la valoración de riesgos en los que cada uno de los riesgos identificados se van a enlazar con las unidades de negocio o departamentos implicados en cada uno de los casos.

COBRA ISO17799 Consultant resulta ser un servicio basado en una base de datos de conocimiento para guiar en los procesos de validación y evaluación de cumplimiento de la norma ISO17799, aportando un conjunto de recomendaciones para el cumplimiento final. A través de un conjunto trabajado de preguntas y respuestas se van a poder:

- Establecer el nivel de cumplimiento de cada una de las diez categorías de la norma.
- Identificar qué controles adicionales van a poder aplicarse para incrementar el nivel de cumplimiento de la norma, y por lo tanto, el nivel de seguridad inherente de nuestros sistemas.
- Generar un informe por un lado comprensible, pero por otro de adecuado nivel profesional que podremos utilizar como herramienta de comunicación interna de nuestro nivel de cumplimiento.

Tiene muchas similitudes con la aproximación de CRAMM, aunque no dispone de tantas contramedidas; por el contrario, sus cuestionarios están muy bien trabajados.

1.3.7. Risk Watch

Se trata de una herramienta basada en un sistema experto (48), que permite:

- La gestión del riesgo (de forma estructurada).
- La generación de informes.
- La obtención de estadísticas, para poder ser utilizadas en una gestión cuantitativa del riesgo (por ejemplo, midiendo el ROI[106]).

(106)En inglés son las siglas de *return of inversion*.

(107)Health Insurance Portability and Accountability Act of 1993 (HIPAA).

Dispone de algunos componentes adicionales, de los que destacaríamos el ComplianceWatch para trabajar en HIPPA[107], banca[108], PCI[109], infraestructuras críticas (*nuclear cybersecurity compliances*[110]).

(108)Public Company Accounting Reform and Investor Protection Act of 2002 (también referenciada como Sarbanes-Oxley) y Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA).

(109)PCI: *payment card industry*.

(110)De acuerdo con CNPIC, los ataques a infraestructuras críticas crecieron un 375 % en España en 2016 (224).

1.3.8. OCTAVE

Ideada en SEI/CMU[111], dispone de una versión escalada para organizaciones de pequeña escala (OCTAVE-S).

(111)Software Engineering Institute, Carnegie Mellon University (225).

Esta metodología se basa en un trabajo en grupo, normalmente en forma de *workshops*, más que en la utilización de una herramienta.

Se estructura en tres fases:

1) Recopilación de información (conocimiento) con un trabajo con personas relevantes en la organización, respecto a activos críticos, amenazas y estrategias de contención y protección.

2) Recopilación de información (conocimiento) con un trabajo con personas gestoras de las operaciones.

3) Recopilación de información (conocimiento) con un trabajo con personas sin responsabilidad en las operaciones ni en la dirección.

Al final del trabajo se obtiene:

- Una política (estrategia) de seguridad.
- Un plan de mitigación.
- Una lista de acciones.

La metodología deriva en por lo menos doce sesiones de trabajo, por lo que es un proceso extenso (49).

1.3.9. CRAMM

Metodología (50) desarrollada en 1985 para la gestión de riesgos en sistemas de información, por el Gobierno británico (quien aún ostenta los derechos a través de Insight Consulting[112]), que tiene su última versión publicada en 2003.

(112)CRAMM son las siglas de CCTA (Central Computer and Telecommunications Agency) Risk Analysis and Management Method.

Como metodología, nos permite trabajar la ISO 17799, y algunas de sus características relevantes son:

- Muy buena gestión cualitativa de la información.
- Buen conjunto de contramedidas para poder ser aplicadas de forma comprensible, tanto en el ámbito tecnológico como en el de las políticas de seguridad.
- Se despliega en un modelo de tres fases:
  - Se revisan los elementos de referencia y de contorno para la definición de un modelo de nuestros activos.
  - Se agrupan los activos para poder identificar sus interrelaciones y dependencias. A partir de aquí se hace un análisis de vulnerabilidades y amenazas y se estima el impacto del riesgo (de forma cualitativa).
  - Se eligen y despliegan las contramedidas.

1.3.10. FIRM

Representa una metodología (51) para la gestión (genérica) de riesgos[113]. Se fundamenta en dos documentos y una herramienta:

[113]En inglés son las siglas de *fundamental information risk management*.

- Una guía de implementación.
- Un documento con material adicional para la implementación del proceso.

Su punto fuerte es el elevado nivel de detalle de la documentación, por lo que resulta muy adecuada como punto de entrada para la gestión de riesgos en nuestras organizaciones si estamos dando nuestros primeros pasos en este ámbito.

1.3.11. FRAP

Metodología[114] ideada por Thomas Peltier, con un enfoque orientado a técnicas para gestionar el riesgo basadas en el coste (buscando la eficiencia en coste).

[114]FRAP: *facilitated risk analysis process*.

Estructurado en:

- Análisis de vulnerabilidades
- Análisis del impacto

- Análisis de amenazas
- Trabajo en grupo con un dinamizador con debates y cuestionarios

Es una metodología muy simple y rápida, adecuada en entornos pequeños, que se integra muy bien con soluciones BIA[115].

(115)En inglés son las siglas de *business impact analysis*.

1.3.12. NIST

Es la institución del Gobierno Federal (52) de los Estados Unidos que centraliza muchos de los procesos y recomendaciones en el ámbito de las tecnologías de la información, y por lo tanto la ciberseguridad, y referente de obligado seguimiento, pues muchas de las recomendaciones están de una u otra forma ligadas a esta institución.

Dos buenos documentos que pueden ser un punto de partida para la gestión del riesgo y de la seguridad[116] son:

(116)Toda la serie 800 hace referencia a guías y recomendaciones de ciberseguridad.

- NIST Special Publication 800-39 (53).
- NIST Special Publication 800-30 (54).

En los que se descompone todo el proceso de gestión en nueve pasos:

1) Caracterización del sistema.

2) Identificación de amenazas.

3) Identificación de vulnerabilidades.

4) Análisis de control.

5) Determinación de probabilidades.

6) Análisis del impacto.

7) Determinación del riesgo.

8) Recomendaciones de controles.

9) Documentación de los resultados.

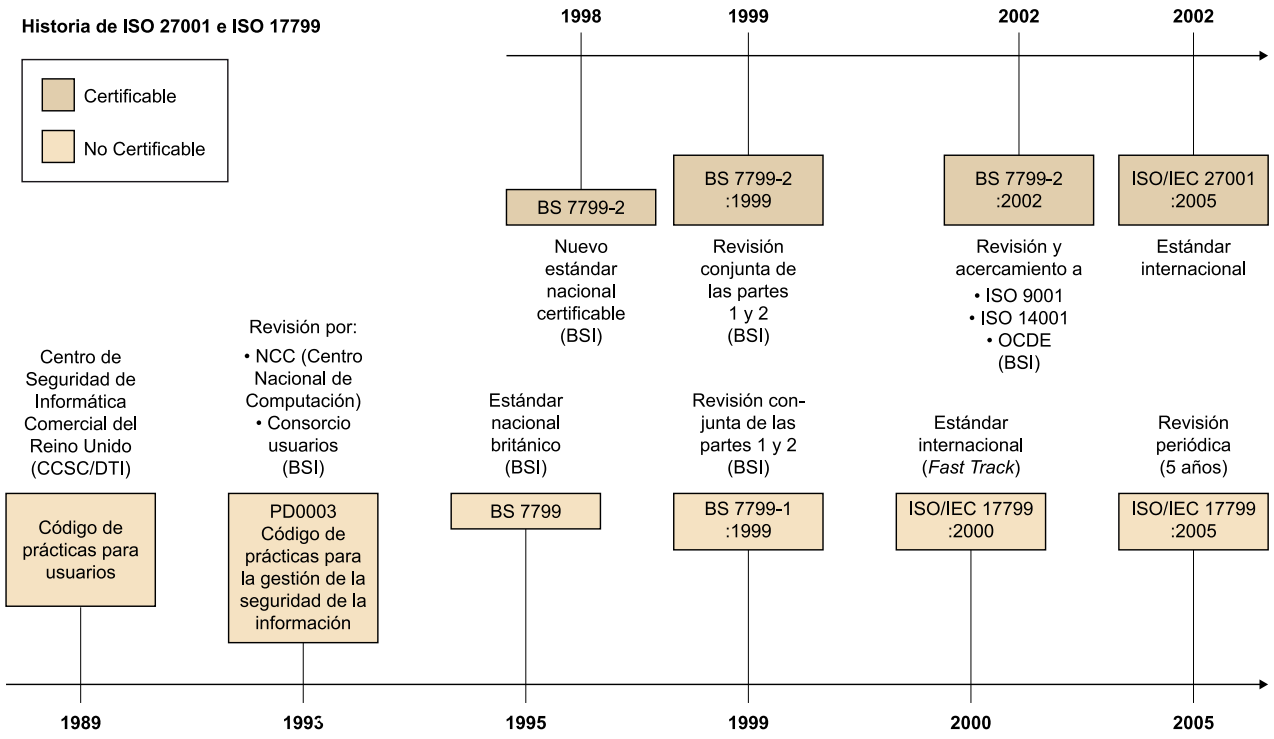
2. Requisitos de un sistema de gestión de la seguridad de la información. ISO 27000

2.1. Visión general de la serie ISO-27000

Pese a que empezó como código de buenas prácticas, o sea, listado de controles (27002), ahora lo importante es el sistema de gestión de la seguridad de la información (27001), y los controles son un anexo.

Actualmente, estamos con la ISO 27001:2013, y en la figura 22 podemos ver la evolución de la serie, desde sus orígenes en el marco de las normas británicas.

Figura 22. Evolución de las normas de gestión de la seguridad de la información



Las principales ventajas que podrían derivar de la implantación de un sistema de gestión de la seguridad de la información son:

1) Aplicar una arquitectura de gestión de la seguridad de la información que identifica y evalúa los riesgos para poder implantar contramedidas eficaces de control y de mejora continuada.

2) Ayudar en la gestión eficaz de la seguridad de la información, evitando, entre otros, inversiones innecesarias, ineficientes o mal dirigidas que se pueden producir para contrarrestar las amenazas (una gestión adecuada y efectiva de las medidas a aplicar, alineadas con el negocio, y dando respuesta real a las amenazas).

3) Aportar una guía para poder:

- Identificar amenazas.
- Implantar controles y contramedidas.
- Establecer responsabilidades, funciones y obligaciones.
- Realizar la formación en seguridad.
- Responder a las incidencias.
- Asegurar la continuidad de las operaciones.
- Regular el uso de la información dentro de los procesos de negocio de la organización.

La serie de la ISO/IEC 27000 incorpora todo un conjunto de normas (55). Es importante saber que las normas no son de libre difusión, sino que deben ser adquiridas (56); también podemos consultar una previsualización del índice de las mismas para mayor confirmación de lo que vayamos a adquirir si tenemos dudas (57).

ISO/IEC 27000: nos permite obtener una visión global (58) del conjunto de normas de la serie, dando para cada una su objetivo y alcance. Nos permite tener el conjunto de definiciones para la serie, y una visión general sobre la importancia de los sistemas de gestión de la seguridad de la información, describiendo el conjunto de fases para la puesta en marcha, monitorización y mejora del sistema de gestión[117].

[(117)]Podemos encontrar la versión en inglés gratuita (226).

Primera versión: mayo de 2009.

Segunda versión: diciembre de 2012.

Tercera versión: enero de 2014.

Cuarta versión: febrero de 2016.

Quinta versión: 2018.

Podemos categorizar el conjunto de normas de la serie, en una serie de agrupaciones, que describimos en los apartados siguientes.

2.1.1. Conjunto de normas para la especificación de requisitos

ISO/IEC 27001

Primera versión: octubre de 2005.

Segunda versión: septiembre de 2013.

Es el punto de partida de toda la serie, definiendo (59) los requisitos del sistema de gestión de la seguridad de la información.

En el anexo A de la norma se enumeran (de forma abreviada) los objetivos de control y los controles que luego se desarrollarán en la norma ISO/IEC 27002, para que de forma rápida en el momento de definir el sistema de gestión de la seguridad de la información de nuestra organización en particular podamos claramente identificar los controles y objetivos de control que debemos implementar y definir. Si bien en el momento de la auditoría no todos son necesarios, sí que se debe siempre justificar la ausencia de algún objetivo de control o de alguno de los controles de la norma ISO/IEC 27002. Como veremos más adelante (capítulo 2), es de importancia que esta norma pueda certificarse.

AENOR ha hecho hasta tres revisiones de la publicación de la norma la última como UNE-ISO/IEC 270011:2013/Cor.2:2015.

ISO/IEC 27006

Primera versión: 1 de marzo de 2007.

Segunda versión: 1 de diciembre de 2011

Tercera versión: 30 de septiembre de 2015.

Especifica (60) los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan sistemas de gestión de la seguridad de la información) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los propios sistemas de gestión de la seguridad de la información. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de

acreditación por sí misma. En España, esta norma no está traducida; sin embargo, sí lo está, para la versión de 2007, en México (NMX-I-041/06-NYCE) y Chile (NCh-ISO27001).

ISO/IEC 27009

Primera versión: 15 de junio de 2016.

No es una norma certificable.

Define los requisitos (61) para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del anexo A. Es de vital importancia para la ampliación de los sectores de aplicación de la norma base.

2.1.2. Conjunto de normas con guías generalistas

ISO/IEC 27002

Primera versión: 1 de julio de 2007.

Segunda versión: septiembre de 2013.

Es la nueva denominación para la norma ISO 17799:2005. Es una guía (62) de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

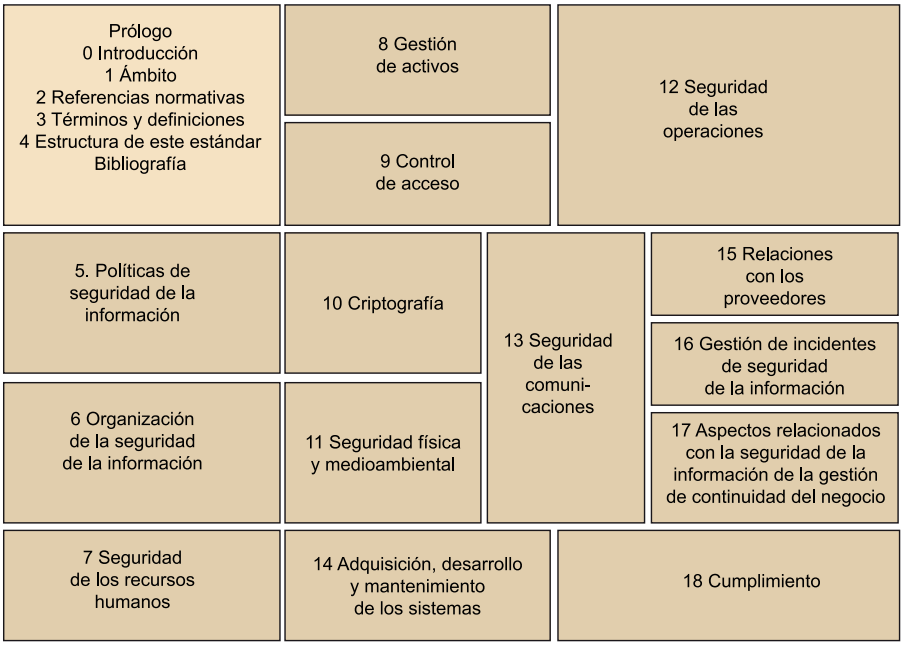
Nuevamente no es certificable.

Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Publicada en España como UNE-ISO/IEC 27002:2009, desde el 9 de diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita).

Actualmente, la última edición de 2013 de este estándar ha sido actualizada a un total de 14 dominios, 35 objetivos de control y 114 controles, que se estructuran en un conjunto de capítulos que tenemos representados en la figura 23.

Figura 23. Estructura de capítulos de la norma ISO27002:2013



ISO/IEC 27003

Primera versión: 2010.

Segunda versión: abril de 2017.

Es una guía (63) para los aspectos de gestión de los sistemas en el entorno de la serie 27000, para dotar de consistencia en su estructura y formato a todos los procesos de gestión de sistemas.

ISO/IEC 27004

Primera versión: 15 de diciembre de 2009.

Segunda versión: diciembre de 2016.

Nuevamente es una norma no certificable.

Es una guía (64) para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un sistema de gestión de la seguridad de la información y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005

Primera versión: 15 de junio de 2008.

Segunda versión: 1 de junio de 2011.

Tercera versión: julio de 2018.

La última versión se ajusta a los requisitos propios de la actualización de la norma ISO/IEC 27001:2013.

Es una norma no certificable.

Proporciona directrices (65) para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

ISO/IEC 27007

Primera versión: 14 de noviembre de 2011.

Segunda versión: 9 de octubre de 2017.

No es una norma certificable.

Es una guía (66) de auditoría de un sistema de gestión de la seguridad de la información, como complemento a lo especificado en ISO 19011.

ISO/IEC TR 27008

Primera versión: 15 de octubre de 2011.

No es una norma certificable.

Es una guía (67) de auditoría de los controles seleccionados en el marco de implantación de un sistema de gestión de la seguridad de la información.

ISO/IEC 27013

Primera versión: 15 de octubre de 2012.

Segunda versión: 24 de noviembre de 2015.

Es una guía (68) de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014

Primera versión: 23 de abril de 2013.

Consiste en una guía (69) de gobierno corporativo de la seguridad de la información.

ISO/IEC TR 27016

Primera versión: 20 de febrero de 2014.

Es una guía (70) de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC 27021

Primera versión: octubre de 2017.

Norma (71) en desarrollo, para incluir los requisitos de las competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información.

2.1.3. Conjunto de normas con guías para sectores específicos de actuación

ISO/IEC 27010

Primera versión: 20 de octubre de 2012.

Segunda versión: 10 de noviembre de 2015.

Consiste en una guía (72) para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a escala nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.

ISO/IEC 27011

Primera versión: 15 de diciembre de 2008.

Segunda versión: diciembre de 2016.

Es una guía (73) de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

ISO/IEC 27017

Primera versión: 15 de diciembre de 2015.

Es una guía (74) de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.

ISO/IEC 27018

Primera versión: 29 de julio de 2014.

Es un código (75) de buenas prácticas en controles de protección de datos para servicios de computación en Cloud Computing.

ISO/IEC 27019

Primera versión: 17 de julio de 2013.

Segunda versión: octubre de 2017.

Guía (76) con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Actualizada como ISO/IEC 27019:2017 para su alineación con ISO/IEC 27002:2013, además de la aplicación a los sistemas de control de procesos (por ejemplo, PLC) utilizados por la industria de la energía para controlar y monitorizar la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor y para el control de los procesos de soporte asociados, también incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en ISO/IEC 27001:2013 a la orientación específica del sector de servicios de energía.

2.1.4. Otras normas

ISO/IEC 27015

Primera versión: 23 de noviembre de 2012.

Es una guía (77) de sistemas de gestión de la seguridad de la información orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

Desde el 24 de julio de 2017 se anuncia que no será actualizada en relación con las novedades de la norma ISO/IEC 27002:2013, aunque sigue disponible para su adquisición por parte de los interesados.

ISO/IEC TR 27023

Primera versión: 2 de julio de 2015.

No es una norma certificable.

Es una guía (78) de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 e ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.

ISO/IEC 27031

Primera versión: 1 de marzo de 2011.

No es una norma certificable.

Es una guía (79) de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

ISO/IEC 27032

Primera versión: 16 de julio de 2012.

Proporciona (80) orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: información de seguridad, seguridad de las redes, seguridad en internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de seguridad cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de seguridad cibernética y un marco que permite a las partes interesadas colaborar en la solución de problemas en la ciberseguridad.

ISO/IEC 27033

Norma (81) en fase de desarrollo, dedicada a la seguridad en redes, consistente en seis partes:

- 27033-1, conceptos generales (publicada el 15 de diciembre de 2009 y revisada el 10 de octubre de 2015);

- 27033-2, directrices de diseño e implementación de seguridad en redes (publicada el 27 de julio de 2012);

- 27033-3, escenarios de referencia de redes (publicada el 3 de diciembre de 2010);

- 27033-4, aseguramiento de las comunicaciones entre redes mediante pasarelas de seguridad (publicada el 21 de febrero de 2014);

- 27033-5, securización de comunicaciones mediante redes privadas virtuales (publicada el 29 de julio de 2013);

- 27033-6, securización de redes IP sin cables (publicada en junio de 2016).

ISO/IEC 27034

Norma (82) parcialmente desarrollada dedicada la seguridad en aplicaciones informáticas, consistente en siete partes:

- 27034-1, conceptos generales (publicada el 21 de noviembre de 2011);

- 27034-2, marco normativo de la organización (publicada el 15 de agosto de 2015);

- 27034-3, proceso de gestión de seguridad en aplicaciones (publicada en mayo de 2018);

- 27034-4, validación de la seguridad en aplicaciones (en fase de desarrollo);

- 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (publicada el 9 de octubre de 2017);

- 27034-6, guía de seguridad para aplicaciones de uso específico (publicada en octubre de 2016);

- 27034-7, marco predictivo de en la seguridad (publicada en mayo de 2018).

ISO/IEC 27035

Primera versión: 17 de agosto de 2011.

Proporciona una guía (83) sobre la gestión de incidentes de seguridad en la información. Consta de tres partes:

- 27035-1, principios en la gestión de incidentes (publicada en noviembre de 2016);

- 27035-2, guías para la elaboración de un plan de respuesta a incidentes (publicada en noviembre de 2016);

- 27035-3, guía de operaciones en la respuesta a incidentes (que tiene parada su definición y concreción).

ISO/IEC 27036

Guía (84) en cuatro partes de seguridad en las relaciones con proveedores:

- 27036-1, visión general y conceptos (publicada el 24 de marzo de 2014);
- 27036-2, requisitos comunes (publicada el 27 de febrero de 2014);
- 27036-3, seguridad en la cadena de suministro TIC (publicada el 8 de noviembre de 2013);
- 27036-4, guía de seguridad para entornos de servicios Cloud (publicada en octubre de 2016).

ISO/IEC 27037

Primera versión: 15 de octubre de 2012.

Es una guía (85) que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de vídeo, redes TCP/IP, entre otros dispositivos, y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

ISO/IEC 27038

Primera versión: 13 de marzo de 2014.

Es una guía (86) de especificación para seguridad en la redacción digital.

ISO/IEC 27039:

Primera versión: 11 de febrero de 2015.

Segunda versión: 28 de abril de 2016 (corrección menor).

Es una guía (87) para la selección, despliegue y operación de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040

Primera versión: 5 de enero de 2015.

Es una guía (88) para la seguridad en medios de almacenamiento.

ISO/IEC 27041

Primera versión: 19 de junio de 2015.

Es una guía (89) para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042

Primera versión: 19 de junio de 2015.

Es una guía (90) con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27043

Primera versión: 4 de marzo de 2015.

Desarrolla (91) principios y procesos de investigación para la recopilación de evidencias digitales.

ISO/IEC 27050

Norma (92) desarrollada en tres partes sobre la información almacenada en dispositivos electrónicos en relación con su identificación, preservación, recolección, procesamiento, revisión, análisis y producción:

- 27050-1, conceptos generales (publicada en noviembre de 2016);
- 27050-2, guía para el gobierno y gestión (en desarrollo);
- 27050-3, código de buenas prácticas (en desarrollo).

ISO/IEC TR 27103:2018

Primera versión: 22 de febrero de 2018.

Norma (93) desarrollada para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.

ISO 27799

Primera versión: 12 de junio de 2008.

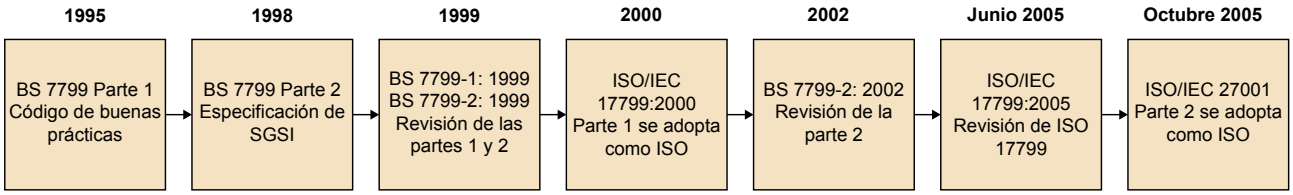
Segunda versión: julio de 2016.

Es una norma (94) que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

2.2. Diferentes versiones

Para poder entender el punto actual de la norma, es conveniente echar una ojeada a la figura 24, donde podemos ver cómo hemos evolucionado en los últimos años, y de dónde viene la norma.

Figura 24. Orígenes de la ISO 27001 hasta 2005



En este ciclo hay tres puntos importantes:

1) Los orígenes con la norma BS 7799[118], que se publicó por primera vez en 1995 para proporcionar a las organizaciones un conjunto de buenas prácticas para la gestión de la seguridad de la información; la primera parte, como vemos, no tiene un proceso de certificación, sino una recopilación de buenas prácticas. No es hasta la aparición de la segunda parte que se establece todo el proceso para la certificación de un sistema de gestión de la seguridad de la información en una organización, incluyendo la certificación por parte de una entidad certificadora independiente.

(118)De la British Standard Institution.

2) La adopción, por parte de ISO, de la norma con la numeración ISO/IEC 17799 en el año 2000, aunque en un primer momento solo se incorporó la primera parte de la norma, pues la segunda parte no acababa de estar adaptada a la filosofía de las normas ISO de sistemas de gestión, en todo su proceso de certificación.

3) Finalmente, en 2005, se incorporó el proceso de certificación en la norma ISO y esta pasó a denominarse ISO/IEC 27001/2005, mientras que la revisión de la ISO/IEC 17799 quedó como norma ISO/IEC 27002:2005.

En marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información[119].

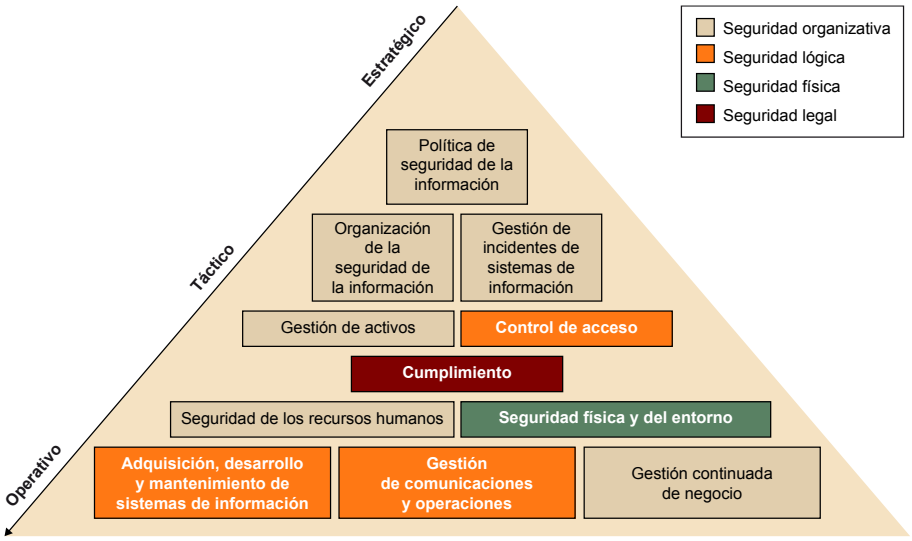
(119)Toda la información disponible públicamente sobre el desarrollo de las normas de la serie 27000 puede consultarse en las páginas web del subcomité JTC1/SC27 (227) (228).

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirven de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie, como hemos visto desglosado en el apartado anterior.

Las dos últimas versiones de la ISO 27001 son la 27001:2005 y la 27001:2013. Veamos los dominios de cada una de las versiones. Empecemos por los dominios de la ISO 27001:2005, que, como vemos en la figura 25, se estructuran en diferentes ámbitos de actuación:

- Política de seguridad de la información.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento en sistemas de información.
- Gestión de incidentes de sistemas de información.
- Gestión continuada de negocio.
- Cumplimiento.

Figura 25. Ámbito de actuación de los dominios de la ISO 27001:2005



Es interesante disponer de un lugar de referencia con la información referente a los dominios en cada una de las dos últimas versiones de la norma. Podemos ver la relación para la norma ISO/IEC 27002:2005 en la figura 26 y la de la norma ISO/IEC 27002:2013 en la figura 27[120].

[120]Puede extenderse el detalle en algunas fuentes (229).

Figura 26. Dominios, objetivos de control y controles ISO/IEC 27002:2005 (229)

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/Controls%20ISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.
6.2 Terceros.
6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.
7.1 Responsabilidad sobre los activos.
7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.
7.2 Clasificación de la información.
7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8.1 Antes del empleo.
8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.
8.2 Durante el empleo.
8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seg. de la informac.
8.2.3 Proceso disciplinario.
8.3 Cese del empleo o cambio de puesto de trabajo.
8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO.
9.1 Áreas seguras.
9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.
9.2 Seguridad de los equipos.
9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.
10.2 Gestión de la provisión de servicios por terceros.
10.2.1 Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.
10.3 Planificación y aceptación del sistema.
10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.
10.4 Protección contra el código malicioso y descargable.
10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.
10.5 Copias de seguridad.
10.5.1 Copias de seguridad de la información.
10.6 Gestión de la seguridad de las redes.
10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.
15.3 Consideraciones sobre las auditorías de los sistem. de información.
15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Ver. 4.0, 16-1-2011

Figura 27. Dominios, objetivos de control y controles ISO/IEC 27002:2013

Los ámbitos de actuación de los dominios son:

- Estratégico.
- Táctico.
- Operativo.

Los dominios de la ISO 27001:2013 son:

- Política de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- **Criptografía, política y gestión de claves.**

- Seguridad física y del entorno.
- **Seguridad de las operaciones.**
- **Seguridad de las comunicaciones.**
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- **Relación con los proveedores.**
- Gestión de incidentes de los sistemas de información.
- **Los aspectos de los sistemas de información en la gestión de la continuidad del negocio (GCN).**
- Cumplimiento.

2.3. ISO 27001:2013

Es auditable, y permite a las empresas superar sus procesos de certificación:

- Mejorar su prestigio hacia sus clientes.
- Dotar de un mecanismo de garantía hacia los trabajadores.
- Garantizar que nuestras actuaciones están alineadas con las actuaciones de las organizaciones punteras desde el punto de vista global.
- Disponer de un mecanismo de obligado cumplimiento.
- Conocer el rumbo hacia el que deseamos llevar la organización.
- Acreditar un reconocimiento mundial.
- Avalar una garantía para datos entregados.

La implantación sigue el flujo habitual de todo sistema de control, estructurado en cuatro fases[121], que vemos reflejadas en la figura 28, con sus subprocesos:

(121)En inglés se utiliza las siglas PDAC: *plan*, *do*, *check*, *act*.

- Planificación, donde definiremos el sistema de gestión de la seguridad de la información, el alcance al que deseamos llegar, las políticas que vamos a poner en marcha, y qué análisis y gestión del riesgo queremos manejar.
- Acción, donde vamos a ocuparnos de la implementación y operación del sistema de gestión de la seguridad de la información definido en la fase anterior; realizaremos e implementaremos las políticas, procedimientos,

procesos y controles definidos, y trabajaremos toda la parte fundamental de concienciación y formación. Es en esta fase en la que se trabaja la gestión del cambio, derivado de la puesta en marcha del sistema de gestión de la seguridad de la información.

- Monitorización, en la que revisaremos los resultados del sistema de gestión de la seguridad de la información, evaluando y midiendo el desempeño de los objetivos y controles, y llevaremos a cabo todos los procesos y procedimientos de auditoría interna.

- Mejora, donde trabajaremos en la identificación de elementos de mejora del sistema de gestión de la seguridad de la información, llevando a cabo acciones tanto correctivas como preventivas de nuestro procesos de auditoría.

Figura 28. Fases de despliegue del sistema de gestión de la seguridad de la información: ISO 27001

Planificación (*Plan*)	**Acción (*Do*)**	**Monitorización (*Check*)**	**Mejora (*Act*)**	**Auditoría de certificación**
1 Diseñar SGSI 2 Analizar procesos 3 Definir alcance 4 Elaborar política de seguridad 5 Identificar y evaluar inventario de activos 6 Realizar análisis de riesgos 7 Generar SOA	8 Generar plan de mitigación de riesgos 9 Aplicar plan de mitigación de riesgos 10 Implementar controles seleccionados 11 Gestionar el proceso de cambio	12 Revisiones generales 13 Revisiones independientes 14 Auditoría interna 15 Revisiones técnicas	16 Implementar mejoras 17 Tomar acciones preventivas y correctivas 18 Comunicar resultados de las acciones tomadas	19 Preauditoría 20 Cierre de no conformidades de la preauditoría 21 Visita inicial entidad certificadora 22 Cierre de no conformidades detectadas 23 Auditoría de certificación entidad certificada

En todo el proceso existe una quinta fase, que normalmente se incorpora en el ciclo, que es la de auditoría (no tiene sentido desplegar todo el ciclo de la ISO 27001 sin plantearse la auditoría y certificación de la misma).

Para cada una de las fases, se definen una serie de procesos estandarizados:

Planificación:

- Diseñar el sistema de gestión de la seguridad de la información.

- Analizar los procesos de la organización a incluir en el mismo.

- Definir el alcance del mismo.

- Elaborar la política de seguridad.

- Identificar y evaluar el inventario de nuestros activos.

- Realizar el análisis de riesgos.
- Generar SOA.

Acción:

- Generar el plan de mitigación de riesgos.
- Aplicar dicho plan de mitigación de riesgos.
- Implementar los controles seleccionados.
- Gestionar el cambio.

Monitorización:

- Revisiones generales.
- Revisiones independientes.
- Auditorías internas.
- Revisiones técnicas.

Mejora:

- Implementar mejoras del sistema de gestión de la seguridad de la información.
- Tomar acciones preventivas y correctivas.
- Comunicar los resultados de las acciones tomadas.

Auditoría:

- Preauditoría.
- Cierre de no conformidades de la preauditoría.
- Visita inicial de la entidad certificadora.
- Cierre de no conformidades detectadas.
- Auditoría de certificación de la entidad certificadora.

2.4. Directrices y métricas

La gestión de riesgos, que supone un proceso cíclico e iterativo, se descompone en seis fases, que representamos en la figura 30:

Fase 1: Definir el alcance del análisis de riesgos. En qué servicios, departamentos, operaciones vamos a proceder a analizar los riesgos. Nos vendrá en cierta forma marcado por la capacidad de actuación que tengamos, en cuanto, por ejemplo, a recursos, tanto económicos como tecnológicos, de personas y de tiempo.

Fase 2: Identificar y valorar los activos. Una vez definido el ámbito de actuación, vamos a tener que identificar los activos que nos ocupan, y una vez identificados estos, los tendremos que poder valorar de alguna forma. Sin la identificación y valoración de activos, nuestro plan de análisis de riesgos no puede nunca ser operativo.

Cada uno de los activos tiene dos elementos de valoración:

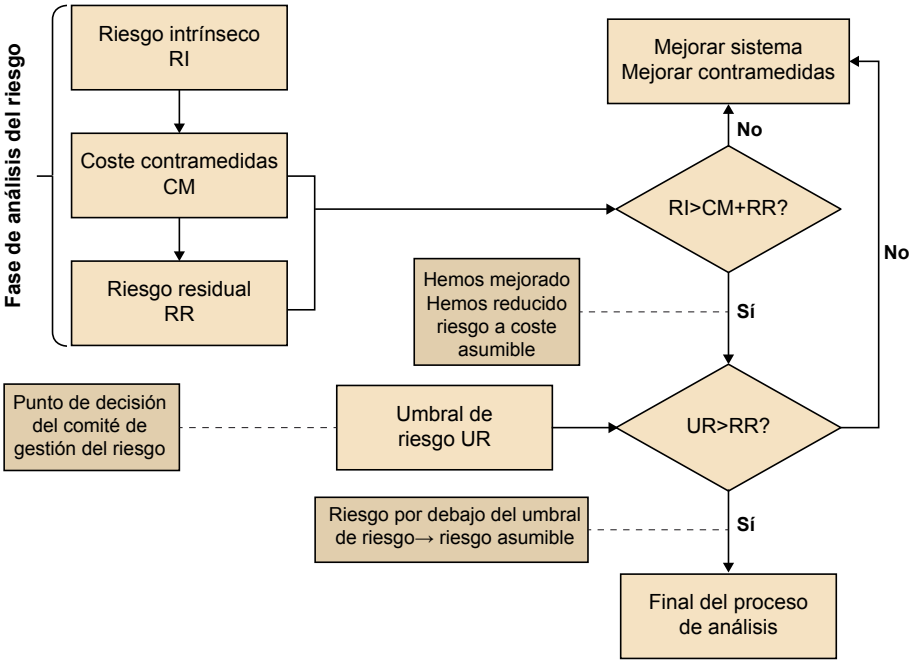
- Intrínseco: que podríamos decir que es el valor actual de mercado del activo.

- Adquirido: que representa para nuestra organización el coste de restitución del activo, en caso de sufrir algún daño, que pueda ser temporal o total.

Por ejemplo, podemos suponer que tenemos impacto sobre la disponibilidad del activo; esta falta de disponibilidad puede ser temporal, por efecto de un ataque de denegación de servicio, que ha saturado el número de conexiones disponibles de un servidor, por ejemplo, o puede ser total, por destrucción del propio activo, por ejemplo, por efecto de un incendio.

Las contramedidas que vayamos aplicando van a influir en el impacto del incidente, o en la probabilidad del ataque; en definitiva, van a tener incidencia en el valor del riesgo estimado, como podemos ver en la figura 29, y por ello el proceso tiene que ser claramente iterativo y continuado.

Figura 29. Ciclo de gestión del riesgo. Riesgo intrínseco, contramedidas y riesgo asumible relacionados



En la figura 29 vemos la relación entre el riesgo intrínseco, las contramedidas aplicadas y el riesgo asumible de la organización en el ciclo continuo de gestión de la seguridad. El valor del riesgo, una vez aplicadas las contramedidas, debe ser:

- Obviamente, inferior al riesgo intrínseco; si no, no habremos conseguido reducir el riesgo.

- Pero debe permitir amortizar el coste de las contramedidas; si no, estaremos reduciendo el riesgo a un coste mayor que la mejora, estaremos matando moscas a cañonazos.

Fase 3: Identificar las amenazas, como siempre relacionadas con los activos que queremos proteger. No se trata de tener listas muy extensas, sino la enumeración de aquellas amenazas que podremos relacionar con nuestros activos.

En esta fase, las amenazas se suelen clasificar para su mejor evaluación, por ejemplo, en tres categorías:

- Desastres naturales: que suelen ser independientes del valor y función en nuestro sistema. La ubicación de la sede de la organización es de importancia para estas amenazas y, por lo tanto, es una consideración que debe hacerse en el momento, muy inicial, de decidir la ubicación física de unas instalaciones. Claramente suelen ser las menos frecuentes, pero tienen un impacto muy elevado[122].

[122]Cuidado con estas afirmaciones sobre la frecuencia. Es poco probable que suframos terremotos, pero por ejemplo las riadas son mucho más frecuentes, o temporales que deriven en inundaciones.

- Accidentes y errores, derivados de personas, equipos o servicios. Son claramente los más frecuentes; siempre hemos de recordar que la amenaza

más frecuente suele ser interna (nosotros mismos somos la más frecuente amenaza a nuestro sistema), y por lo tanto es vital el despliegue de mecanismos de control, prevención y auditoría de todos nuestros procesos.

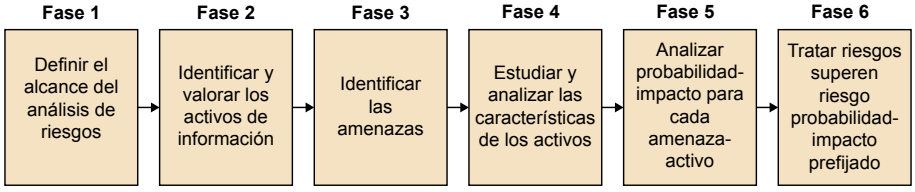
- Ataques: que pueden tener causas muy diversas. Algunos son activos (se buscaba claramente el ataque como respuesta a algo); otros son pasivos (no buscan el ataque, sino que suelen ser más observadores, para la captación de información que se utilizará en posteriores ataques). Evidentemente, la fuente de ataque puede ser interna o externa; es mucho más frecuente (65 %) la interna respecto a las externas.

Fase 4: Estudiar y analizar las características de nuestros activos. Esta fase es importante, para poder conocer los puntos débiles que podamos tener, y también para poder relacionar activo, con amenazas, y conocer impacto.

Fase 5: Emparejar los activos con las vulnerabilidades. Cada activo ha de tener vulnerabilidades asociadas, y no podemos tener vulnerabilidades sin ningún activo asociado; si fuera el caso, nos indicaría que hemos incluido una vulnerabilidad que estaba fuera del ámbito de nuestro proyecto actual de análisis de riesgos. A continuación, hemos de valorar la probabilidad de que cada una de las vulnerabilidades asociadas a cada activo se produzcan; al mismo tiempo, en caso de producirse, hemos de poder valorar el impacto que van a tener, medido como impacto sobre el negocio[123].

(123)Todo plan de gestión de la seguridad está dirigido a mitigar los riesgos que pueden tener impacto en nuestro negocio.

Figura 30. Fases de gestión de riesgos



Para cada uno de los riesgos, además de emparejar vulnerabilidades con los activos, hemos de identificar quién es el propietario del activo, como elemento importante de la valoración del impacto.

Fase 6: Tratar los riesgos que sean más relevantes. En esta fase, debemos fijar los umbrales de actuación sobre la base de los cuales vamos a actuar.

En esta fase hemos de elegir los controles que vamos a implantar para tratar los riesgos. Como mínimo, debe incluirse los del anexo A (27002).

Para todos los riesgos que hemos identificado, independientemente de si los vamos a tratar o no, hemos de incluir una declaración de aceptabilidad[124], donde justificaremos si hacemos frente al riesgo o no, siempre de forma contrastable.

(124)En inglés se utiliza el término *statement of acceptance* (SoA).

En cualquiera de las dos opciones, es necesario pasar por el comité de seguridad para la aprobación del propietario del riesgo, y la dirección de la organización.

2.5. Auditoría y control

Los mecanismos de control mínimos que deben implantarse en el momento de desplegar la ISO 27000 son los reflejados en el anexo A de la ISO 27002, que podemos identificar en los catorce dominios representados en la figura 31, y que vamos a analizar en los siguientes apartados.

Figura 31. Dominios de aplicación en el anexo A de la ISO 27002

2.5.1. Política de seguridad

La política de seguridad establece el compromiso de la dirección de la organización y el enfoque de la organización para gestionar la seguridad de la información.

La dirección ha de establecer, de forma clara, las líneas de la política de actuación y ha de manifestar su apoyo y compromiso con la gestión de la seguridad de la información.

La política será, una vez definida, distribuida dentro de la organización llegando a todos los destinatarios de una forma que sea apropiada, entendible y accesible en todo momento.

El objetivo de la política de seguridad es, pues, dirigir y dar soporte a la gestión de la seguridad de la información en la organización.

2.5.2. Organización de la seguridad

La estructura de la seguridad realiza la gestión de las acciones relativas a la implantación de los procesos de seguridad de la información dentro de la organización, así como el control y la supervisión periódica de la situación en la que se encuentran los principales indicadores de seguridad.

Esta función implica, pues, la gestión de todas las responsabilidades relativas a la seguridad de la información, por ejemplo, las responsabilidades llevadas a cabo por personal interno a la organización, y las llevadas por personal externo a la organización.

El objetivo principal será gestionar la seguridad de la información dentro de la organización.

2.5.3. Seguridad de recursos humanos

Normalmente, se establecen tres niveles de actuación en cuanto a la seguridad de los recursos humanos:

Contratación: se establecen las responsabilidades de seguridad a poner en conocimiento de los empleados y colaboradores externos. Todo contrato debe incluir aspectos de gestión de la seguridad de la información en la organización, con las responsabilidades de cada una de las posiciones, y con las obligaciones y penalizaciones asociadas en término de seguridad. Toda persona de la organización, en el momento de incorporarse a la organización, debe ser consciente de la importancia que la gestión de la seguridad de la información tiene para la organización.

Relación laboral: se han de establecer todas las pautas y procesos de seguridad que deben seguirse por parte de cada uno de los puestos de trabajo de la organización. Todo proceso de la organización debe tener en consideración los aspectos de gestión de la seguridad de la información.

Finalización: se han de establecer las pautas y los procesos en materia de seguridad de la información relacionados con la finalización de contrato de los empleados y colaboradores externos de la organización. Deben estar claramente definidos para cada puesto de trabajo cuáles son los procesos con los que está relacionado, para, en el momento de finalización de la relación contractual, garantizar que no queda ningún permiso activo que pueda en el futuro tener un impacto negativo en la seguridad de la información de la organización.

El objetivo principal será asegurar que los empleados y colaboradores externos de la organización tienen un claro conocimiento de sus responsabilidades, en todo lo relacionado con la gestión de la seguridad de la información de la organización.

2.5.4. Gestión de activos

Los activos que hemos de proteger han de identificarse y clasificarse. Para cada activo, vamos a definir las medidas de protección más adecuadas en función del nivel de sensibilidad o criticidad, grado de confidencialidad con el que hemos previamente clasificado cada activo dentro de la organización.

Sin identificación ni clasificación no podemos gestionar los activos de la organización.

Se han de definir los propietarios de la información; la responsabilidad sobre los activos ayuda a asegurar a mantener el nivel de protección adecuada sobre los activos.

El objetivo principal será, pues, mantener una protección sobre los activos de la organización con el nivel adecuado en función de su grado de criticidad.

2.5.5. Control de accesos

Se van a establecer los requisitos y las medidas para restringir el acceso sobre la información sensible, y los sistemas que la gestionan de la organización.

El acceso a la información se ha de limitar con el objeto de que los usuarios tengan acceso, única y exclusivamente, a la información que es necesaria (e imprescindible) para el adecuado desarrollo de las funciones profesionales que son propias de sus puestos de trabajo, de acuerdo a la definición de seguridad de la información definidas en el ámbito de seguridad de los recursos humanos.

Los niveles de acceso deben estar actualizados y responder a las necesidades de cada momento: ni más ni menos, ni demasiado pronto, ni demasiado tarde, ni por menos tiempo del requerido, ni durante más tiempo. Todo en su justa medida. Aquí, nuevamente, la relación de la gestión de la seguridad de los recursos humanos con los aspectos de contratación y finalización es primordial para garantizar la adecuada gestión de la seguridad de la información en la organización.

Se ha de establecer el principio de responsabilidad de las acciones realizadas por cada usuario de la organización y de los sistemas de información de la organización mediante sus credenciales de acceso. Las credenciales de acceso no deben compartirse bajo ninguna razón. En este aspecto, la formación en gestión de seguridad de la información de todos los empleados y colaboradores de la organización es de vital importancia, así como todos los aspectos relacionados con los avisos de seguridad (especialmente, los de acceso a los sistemas).

El objetivo será controlar y restringir el acceso a la información y a los sistemas de gestión de la información de la organización.

2.5.6. Cifrado

Se van a establecer los requisitos para los procesos de cifrado, tanto para los aspectos de controles de autenticación como de integridad, como podrían ser las firmas digitales (y su gestión) o los mecanismos de autenticación de mensajes, o la gestión de las claves criptográficas.

2.5.7. Seguridad física y del entorno

Se han de establecer los controles de seguridad física a implementar sobre los sistemas de procesamiento de la información para la prevención de accesos no autorizados. En este ámbito, podemos incluir la definición de áreas de seguridad, barreras de acceso, perímetros de seguridad…

Se establecen también las medidas de protección física y ambiental del equipamiento frente a los riesgos derivados, entre otros, de desastres naturales, accidentes, sabotaje o vandalismo.

El objetivo será prevenir accesos no autorizados, daños o interferencias en las instalaciones, equipamientos y sistemas de la organización.

2.5.8. Seguridad en la operación

Se establecen los niveles de servicio, las funciones y las responsabilidades relativas a la operación de la información, buscando la gestión de los recursos de forma eficaz y eficiente.

Se definen los procesos y pautas que han de garantizar la integridad y disponibilidad de la información.

Se han de investigar vulnerabilidades, amenazas y riesgos de seguridad relacionados con la operación de la información.

El objetivo será asegurar la correcta y segura operación y gestión de los datos y de la información de los sistemas de procesamiento de la información.

2.5.9. Seguridad en las telecomunicaciones

Se establecen los niveles de servicio, las funciones y las responsabilidades relativas a la comunicación de la información, buscando la gestión de los recursos de forma eficaz y eficiente, garantizando en todo momento su integridad y disponibilidad.

Se definen los procesos y pautas que han de servir para monitorizar la seguridad que existe en las redes de comunicaciones de información de la organización.

Se han de investigar vulnerabilidades, amenazas y riesgos de seguridad relacionados con la comunicación de la información.

El objetivo será asegurar la correcta y segura comunicación de información de los sistemas de la organización.

2.5.10. Desarrollo y mantenimiento de sistemas

Se van a establecer los requisitos de seguridad e integridad necesarios que deben tenerse en cuenta en los sistemas de información que se desarrollan, se mantienen o se adquieren.

La seguridad debe estar presente en todas las fases de desarrollo, de mantenimiento o de adquisición, de los sistemas de procesamiento de la información. La prevención, a través de la adecuada inversión en las fases iniciales, por ejemplo, de definición de necesidades y requerimientos, tiene un gran retorno en la seguridad derivada frente a la reacción por tener que actuar *a posteriori*.

Es vital disponer de los procesos y pausas de control de calidad y seguridad en relación con los sistemas de información de la organización.

El objetivo será garantizar el procesamiento seguro de la información y, en consecuencia, la integridad, confidencialidad y disponibilidad de la misma, en relación con los sistemas de procesamiento de información de la organización.

2.5.11. Relaciones con proveedores

Se van a indicar las recomendaciones orientadas a la protección de la información de una organización cuando esta entra en colaboración con sus proveedores; por lo tanto, se van a dar los procedimientos, políticas y guías de uso para este objetivo.

Cuando tengamos servicios que se den por parte de proveedores nuestros a terceros, hemos de tener bien definidos los mecanismos de control y monitorización de los mismos, claramente establecidas las pautas de auditoría de los mismos, y muy bien definidos los contratos de garantía de servicios con nuestros proveedores.

2.5.12. Gestión de incidentes de seguridad

Cualquier incidente de seguridad de la organización puede quedar identificado por parte de cualquier empleado o colaborador externo de la organización, y debe ser comunicado de forma inmediata.

Se ha de disponer de un procedimiento de gestión y escalado de los incidentes de seguridad con el objeto de garantizar una respuesta adecuada a los mismos de forma lo más rápida, fiable y efectiva posible.

La organización ha de aprender de los incidentes de seguridad, y actuar de forma coherente cuando se produzcan, para procurar que no vuelvan a producirse en el futuro. Todo incidente de seguridad ha de entenderse como una oportunidad para mejorar los controles y procesos de seguridad de la información definidos para que dicho incidente no pueda volver a producirse. Incidentes menores pueden representar la oportunidad de detectar problemas que puedan ser de importancia en incidentes de mayor impacto.

La gestión de los incidentes de seguridad está íntimamente relacionada con el despliegue de un sistema de monitorización de incidencias, pero sobre todo con un sistema de registro e identificación de los incidentes de seguridad que se vayan produciendo.

El objetivo será asegurar la identificación de todos los incidentes de seguridad que se puedan producir y gestionar la respuesta que se debe dar a ellos de forma adecuada.

2.5.13. Continuidad de negocio

El proceso de gestión de la continuidad de negocio minimiza el impacto que se pueda producir en la organización cuando se produce un incidente de seguridad, y ayuda a recuperarse frente a una interrupción o pérdida parcial o total de los sistemas de procesamiento de la información en la organización.

Nos debe permitir identificar los procesos de negocio clave y los sistemas de procesamiento de la información críticos, y por lo tanto, en los que deben focalizarse los esfuerzos y la inversión para garantizar la continuidad del negocio de la organización.

Ha de implicar el desarrollo de planes alternativos de gestión de los procesos de negocio mientras se estén llevando a cabo las medidas necesarias para recuperar los sistemas de procesamiento de la información afectados por un incidente de forma rápida y fiable.

El objetivo principal será garantizar la continuidad de las operaciones del negocio frente a interrupciones de los sistemas de procesamiento de la información y asegurar una adecuada, en tiempo y forma, resolución de los fallos e incidentes producidos.

2.5.14. Cumplimiento normativo

El diseño, operación, uso y gestión de los sistemas de información de la organización puede ser objeto de requisitos legales específicos, en muchos campos de actuación de la organización (por ejemplo, salud, alimentación, servicios, banca, comercio, transporte, educación...).

Nos debe permitir identificar posibles incumplimientos contractuales o reguladores cuando se opera en diferentes circunscripciones y jurisdicciones.

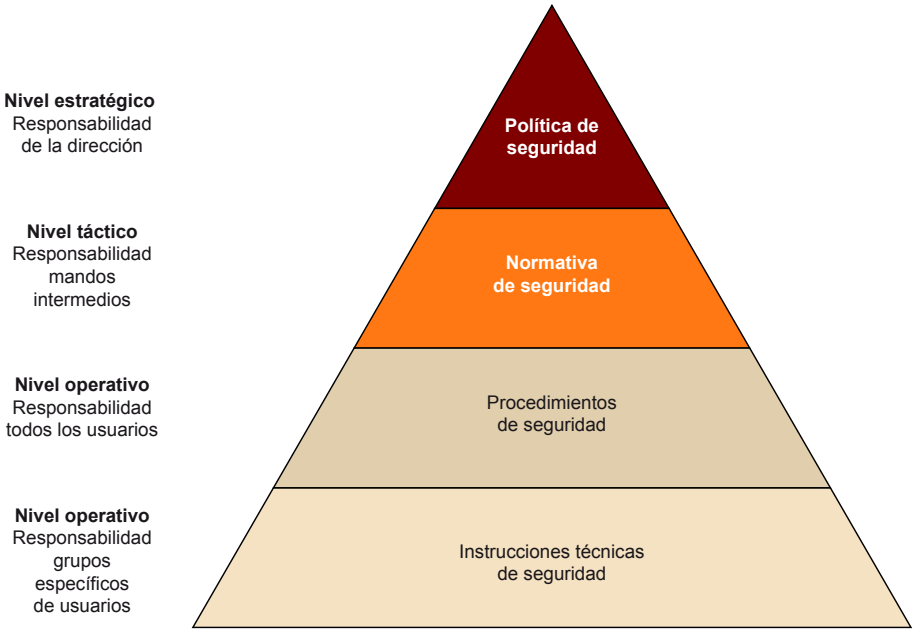
Es imprescindible disponer de un asesoramiento legal y jurídico en el ámbito de gestión de la seguridad de la información.

El objetivo será garantizar el cumplimiento del marco legal (y operacional) de la organización y todas las jurisdicciones en las que opere.

2.6. Mecanismos de gestión de la ISO 27000

Para que el despliegue de la ISO 27000 sea efectivo (como en todos los mecanismos de gestión de la seguridad), es imprescindible la implicación de la (alta) dirección de la organización, tal y como representamos en la figura 32.

Figura 32. La política de seguridad debe ser aprobada por la dirección



La política de seguridad debe ser aprobada por la dirección

Para que el despliegue funcione, además de la implicación y aprobación de la política de seguridad por parte de la dirección, necesitamos un órgano ejecutivo de control y seguimiento de todas las acciones y procedimientos a definir e implantar; es el comité de seguridad de la información, que tiene por función principal:

- Velar por la seguridad de la información y de los activos de la organización.
- Evaluar y promocionar el sistema de gestión de la seguridad de la información en la organización.
- Atender las posibles amenazas e incidencias de seguridad.
- Asegurar que los cambios en la organización se reflejan en el propio sistema de gestión de la seguridad de la información.

La composición del comité variará en función del propio organigrama de cada organización, pero suele ser recomendable que lo formen (si existe la figura en la organización):

- Responsable de seguridad (CISO).
- Responsable de sistemas (CIO).
- Responsable de riesgos.
- Responsable de operaciones.

Pueden ser opcionales:

- Responsable de recursos humanos.
- Responsable comercial (director comercial).
- Responsable de marketing y comunicaciones.
- Responsable financiero.

Como resultado de las actuaciones que vamos a definir, tendremos un plan de acciones a desplegar, que garantizaremos que está avalado por el comité.

Cada una de las acciones se concretará en forma de proyectos, que deberán tener su planificación asociada, como vemos en la figura 33.

Figura 33. Proyectos a desplegar y su temporalidad en el plan de acciones

PROYECTOS	Q1	Q2	Q3	Q4	Q5
1.- REALIZACIÓN DEL ANÁLISIS DE RIESGOS/GESTIÓN/ACEPTACIÓN					
2.- ELABORACIÓN DE LA POLÍTICA DE SEGURIDAD					
3,. CREACIÓN ESTRUCTURA ORGANIZAATIVA QUE GESTIONE EL PLAN (COMITÉ DE SEGURIDAD)					
4.- MEJORAR ASPECTOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN					
5.- MEJORAR LA RESPONSABILIDAD SOBRE LOS ACTIVOS					
6.- ESTABLECER UNOS NIVELES DE CLASIFICACIÓN PARA LA INFORMACIÓN					
7.- PERSONAL→CONTRATACIÓN					
8.- PERSONAL→EN LA ORGANIZACIÓN					
9.- PERSONAL-→FIINALIZACIÓN					
10.- PROCEDIMIENTOS A REALIZAR PARA LA BAJA DE EQUIPOS					
11.- DOCUMENTAR PROCEDIMIENTOS DE OPERACIÓN Y RESPONSABILIDADES					
12.- CREAR PLANES DE CAPACIDAD DE LOS SISTEMAS DE INFORMACIÓN					
13.- MEJORAR LA MONITORIZACIÓN					
14.- DOCUMENTAR LOS REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESO					
15.- ASEGURAR LA SEGURIDAD DE TODOS LOS SISTEMAS DE INFORMACIÓN					
16.- REALIZAR AUDITORÍAS PARA DETECTAR VULNERABILIDADES TÉCNICAS					
17.- CREAR UN PLAN DE CONTINUIDAD DEL NEGOCIO					
18.- ESTABLECER POLÍTICAS DE REALIZACIÓN DE LAS AUDITORÍAS TÉCNICAS					
19.- REALIZAR AUDITORÍAS TÉCNICAS INTERNAS Y EXTERNAS					

En su implementación sobre la base de la ISO27002, cada una de las acciones (proyectos) debe tener su ficha, como la de la figura 34.

Figura 34. Ficha de acción sobre la base del anexo A de la ISO27002

ACCIÓN	MEJORAR LA MONITORIZACIÓN DE LAS ACCIONES QUE REALIZA EL PERSONAL			
ISO-27002	A10. GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES			
OBJETIVO	CONTROLAR LOS REGISTROS (LOGS) DE LOS SISTEMAS DE INFORMACIÓN QUE PERMITAN UNA MONITORIZACIÓN DE LAS ACCIONES QUE REALIZA EL PERSONAL DE LA ORGANIZACIÓN RESPECTO AL ACCESO A ACTIVOS DE INFORMACIÓN CRÍTICOS			
DESCRIPCIÓN	CLASIFICACIÓN			
LOS SISTEMAS DE MONITORIZACIÓN PERMITEN ANALIZAR TENDENCIAS, ASÍ COMO ANALIZAR EVIDENCIAS DE LAS ACCIONES QUE REALIZA EL PERSONAL DE LA ORGANIZACIÓN Y DETECTAR POSIBLES USOS INDEBIDOS DE LOS ACTIVOS DE INFORMACIÓN CORPORATIVOS QUE TENGAN ASIGNADO UN GRADO DE CRITICIDAD MAYOR A TENER EN CONSIDERACIÓN: 1.- DEFINIR UNA POLÍTICA DDE REVISIÓN DE LOS REGISTROS DE LOS SISTEMAS DE INFORMACIÓN DE LOS ENTORNOS CORPORATIVOS QUE GESTIONEN INFORMACIÓN CRÍTICA 2.- DOCUMENTAR EL PROCEDIMIENTO DE REVISIÓN DE LOS REGISTROS DEFINIDOS EN LA POLÍTTICA ANTERIOR 3.- REALIZAR ANÁLISIS PERIÓDICOS DE ESTOS REGISTROS PARA ESTUDIAR LAS ACCIONES EFECTUADAS 4.- DISPONER DE SISTEMAS QUE CENTRALICEN TODAS LAS EVIDENCIAS (LOGS) QUE GENERE ESTA MONITORIZACIÓN , Y EN CASO QUE SEA NECESARIO, PUEDAN GENERAR ALARMAS PROACTIVAS BASADAS EN EL ANÁLISIS DE LOS REGISTROS CENTRALIZADOS CON CORRELACIÓN DE EVENTOS DE MANERA TEMPORAL (SINCRONIZACIÓN DE RELOJES) 5.- ESTOS REGISTROS REQUIEREN DE UNA PROTECCIÓN ESPECIAL CON EL FIN DE GARANTIZAR QUE NO SE PUEDEN MODIFICAR POR AQUEL PERSONAL QUE NO SEA INHERENTE A LA ORGANIZACIÓN	ESFUERZO			ALTO
	PRIORIDAD		MEDIA	
	EJECUCIÓN			PRIOR ITARIA
	REQUISITOS	- DISPONER DE LA LISTA DE SISTEMA DE INFORMACIÓN QUE GESTIONAN ACTIVOS CRÍTICOS - - DISPONER DE LA LISTA DE PERSONAL CON RESPONSABILIDADES DE GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN		

Para que el sistema de gestión de la seguridad de la información sea efectivo, es necesario definir un marco normativo interno, con un triple enfoque:

1) Por un lado, la política de seguridad, como herramienta para documentar los principios que sigue la organización respecto a los procesos y elementos que determinan la seguridad de la información y sus sistemas de procesamiento en el ámbito y alcance fijado por el sistema de seguridad.

- La información ha de ser considerada como el activo fundamental de la organización. Por tratarse de un recurso corporativo, debe promoverse y facilitarse su uso compartido por quienes precisen de la información para el ejercicio de sus funciones.

- Todos los miembros de la organización deberán garantizar la confidencialidad, integridad y disponibilidad de la información y los activos asocia-

dos, asegurando en todo momento la continuidad del negocio de la organización.

- El uso no autorizado de la información de la organización, su pérdida o el hecho de provocar su indisponibilidad puede perjudicar seriamente las actividades o la imagen de la organización.

- La dirección de la organización debe tomar las medidas para satisfacer las disposiciones legales, y proteger en todo momento la información frente a accidentes y situaciones erróneas o malintencionadas en su contra.

2) Por otro lado, la normativa de seguridad como herramienta para establecer formalmente los aspectos puntuales relacionados con los requerimientos y las necesidades de seguridad, que serán desarrollados con mayor nivel de detalle en la normativa de seguridad que respaldará la política de gestión de la seguridad de la información corporativa.

Las normas internas de la organización establecen las obligaciones, en materia de seguridad de la información, y desarrollan al detalle la declaración de intenciones en materia de seguridad de la información, es decir, cómo se realiza la política de seguridad de la información.

Los objetivos de seguridad de información se plasman en su mayor medida en las normas de seguridad corporativa.

Algunos ejemplos de normas podrían ser:

- Seguridad básica para el procesamiento de la información.

- Uso de recursos automatizados.

- Uso de recursos no automatizados.

- Clasificación de activos.

- Gestión de riesgos.

- Cumplimiento normativo.

- Divulgación de información corporativa al exterior a través de canales preestablecidos.

3) Y por último, los procedimientos e instrucciones técnicas, como herramientas para identificar las guías de actuación que nos van a garantizar el cumplimiento de lo establecido por las normativas internas en materia de seguridad, que se habrán estructurado en forma de procedimientos e instrucciones de seguridad.

a) Los procedimientos de seguridad de la información son el conjunto de acciones dirigidas a la consecución de una meta o fin. En ellos vamos a identificar las responsabilidades de los usuarios en materia de seguridad de la información, en forma de:

- Responsabilidades globales, que afectan a todos los usuarios de la información.
- Responsabilidades específicas, que afectan a determinados perfiles y roles dentro de la estructura de la organización.

Algunos ejemplos de procedimientos podrían ser:

- Gestión de usuarios y contraseñas.
- Gestión de copias de seguridad.
- Gestión de soportes de datos (sistemas de almacenamiento).
- Ejercicio de los derechos «ARCO».
- Gestión de incidentes de seguridad.
- Gestión de cambios.

b) Las instrucciones técnicas de seguridad buscan establecer los requisitos técnicos y las configuraciones de la infraestructura que está disponible en la organización con el objeto de garantizar la seguridad de la información.

Algunos ejemplos de instrucciones técnicas podrían ser:

- Configuración del sistema SAP/R3.
- Configuración de Atlantis.
- Configuración del antivirus.
- Especificaciones de la caja de seguridad.
- Requisitos del sistema de extinción de incendios.

- Configuración de cortafuegos.
- Algoritmos de cifrado.
- Sistemas ambientales.

La representación gráfica de estos tres niveles se puede ver en la figura 32, en la que vemos cómo pasamos por los diferentes niveles de decisión de la organización: de lo estratégico con la política de seguridad, pasando por el táctico con la normativa de seguridad, para acabar en el operativo con los procedimientos de seguridad y las instrucciones técnicas de seguridad. Los procedimientos son de aplicación para todo el personal de la organización, cada uno en su ámbito, obviamente, mientras que las instrucciones técnicas son de aplicación por parte del personal con responsabilidades técnicas en sus puestos de trabajo.

A través de estos diferentes niveles de actuación se irá desplegando el plan de acciones de nuestro sistema de gestión de la seguridad de la información de nuestra organización.

La información de nuestra organización deberá identificarse y clasificarse, para poder posteriormente ser tratada de forma conveniente.

Las medidas de protección de la información están siempre directamente relacionadas con el nivel de confidencialidad con el que, previamente, habremos clasificado cada uno de los activos de información.

La información que se gestiona se clasifica en función de sus requisitos de confidencialidad, integridad y disponibilidad, así como en función del impacto (financiero, por ejemplo) que implicaría una pérdida, corrupción, robo o indisponibilidad de la misma.

Por ejemplo, se pueden definir cuatro niveles, como vemos en la figura 35:

Nivel 0: Información de uso interno y externo cuya pérdida o acceso no autorizado no tiene ningún impacto negativo en la organización.

Nivel 1: Información de uso interno exclusivo cuya pérdida o acceso no autorizado podría ocasionar una situación embarazosa para la organización.

Nivel 2: Información de uso interno y externo cuyo acceso está sujeto a autorización previa y cuya distribución debe ser controlada. La pérdida o acceso no autorizado dañará considerablemente la organización.

Nivel 3: Información de alto nivel de confidencialidad cuya pérdida o acceso no autorizado podría tener un impacto muy elevado en los intereses de la organización, incluida su propia supervivencia.

Figura 35. Clasificación del nivel de riesgo de la información en cuatro niveles

Como se ve, la clasificación del nivel de riesgo de la información tiene un gran contenido subjetivo, aunque se tratará de disponer de métricas que ayuden a objetivar la clasificación.

Los tres aspectos fundamentales de la información que se procura proteger en el despliegue de la ISO 27000 son la confidencialidad, la integridad y la disponibilidad.

La confidencialidad, entendida como la propiedad de prevenir la divulgación de información a personas, ya sean internas o externas de la organización, que, por diversos motivos, no tienen autorización para conocerla.

La integridad, entendida como la propiedad de mantener la información libre de modificaciones no autorizadas, asegurando que tanto dicha información como sus procesos y métodos de procesamiento son exactos y completos.

La disponibilidad, entendida como la propiedad de garantizar que la información está a disposición de ser utilizada en el momento y forma que un usuario autorizado lo requiera.

Con tal de garantizar la integridad de la información, es importante mantener estos cinco simples criterios:

- No información innecesaria. Almacenar solo la información que sea necesario en función de los requisitos operativos y normativos de la organización (cuanta más información debe tener garantizada su integridad, más costoso y complejo será para la organización).

- No información duplicada. Almacenar solo la información en ficheros maestros, evitando de esta forma la posibilidad de disponer de duplicados no controlados de la información. No confundir con el proceso de copias de seguridad de los sistemas de almacenamiento de la información, sino más bien se trata de garantizar que todos los usuarios están trabajando con los mismos ficheros maestros (centralizados) de información. La mejor manera de evitar duplicidades que luego no vamos a controlar es

prohibir las copias de la información en determinados sistemas de fichero de destino.

- No información incorrecta. La información almacenada será exacta y reflejará de forma fiel la situación de la organización.

- No información desordenada. Los mecanismos de almacenamiento de la información han de garantizar el orden y la clasificación de la información, y han de permitir su identificación de forma inequívoca.

- No información falsa. La modificación de la información en los ficheros y archivos maestros solo podrá ser realizada por personal autorizado de la organización.

Con tal de garantizar la disponibilidad de la información, es importante mantener estos tres simples criterios:

- Sí información compartida. La información de la organización deberá estar disponible en todo momento y será compartida entre todos los usuarios con permisos de acceso de la organización. Se realizará una copia de seguridad de los datos tras cada actualización, con el objeto de disponer de un conjunto de información lo más actual posible, en caso de pérdida de los ficheros maestros. Es una buena política de seguridad hacer copias diarias de la información.

- No información en desuso. En los ficheros maestros, no debe mantenerse ninguna información que no esté actualizada. Las informaciones no actualizadas deben mantenerse solo en las copias de seguridad del pasado. Cuanta menos información debamos gestionar, más fácil nos será garantizar su disponibilidad. La disponibilidad de la información es cara, pues los sistemas de almacenamiento que tienen mayores niveles de garantía de disponibilidad son más pequeños y más caros.

- Información en el momento justo[125]. La información debe estar al alcance de los usuarios con permisos adecuados en el momento que hagan la petición. No pueden dilatarse en el tiempo los procedimientos de acceso y entrega de información a los usuarios.

(125)En inglés se utiliza el término *just in time*.

Para la gestión de la confidencialidad de la información, es importante conservar solo la información necesaria para el negocio. Es importante entender que la información pasa de ser necesaria a no serlo. En este momento hemos de hacer lo siguiente:

- Destruir la información que está (estaba) clasificada como confidencial (de alto riesgo).

- Reciclar la información que no está (estaba) clasificada como confidencial (de riesgo inexistente). El proceso de reciclado es más rápido y económico, pero solo debe emplearse con información sin ningún tipo de riesgo asociado.

3. La seguridad en sistemas y redes de control y automatización de procesos industriales

3.1. Evolución de la ISA 99

En 1945, se fundó la Sociedad Internacional de Automatización (ISA) (95). Actualmente, es una organización no gubernamental con más de cuarenta mil afiliados distribuidos por todo el mundo. Se encarga del desarrollo de estándares, de la certificación de profesionales para la industria, de la puesta en marcha de programas de formación, de la publicación de libros y artículos técnicos, y promueve conferencias y ferias internacionales en el sector industrial de la automatización.

Distribuye su actividad en diferentes ámbitos (todos en automatización industrial), que por ejemplo podrían clasificarse (de acuerdo a su propia página web) (96) como[126]:

(126)La referencia de todos los ámbitos de actuación sirve de marco para entender la amplitud de sectores en los que aplica la norma. Puede no revisarse detalladamente la lista.

1) Gestión de activos e integración industrial

Cómo se pasa del diseño de una planta de producción, una planta industrial, a su operación y mantenimiento es un proceso que debe gestionarse de forma adecuada para garantizar el éxito final. En todo el proceso, la integración es un elemento clave. Es objeto de este ámbito la optimización de la planta, la optimización de los sistemas de control y la optimización de los activos, pues, además de ser operativa y sostenible, debe llevarse a cabo todo ello de forma lo más óptima posible. En todo proceso de optimización e integración, es clave la forma en la que se gestionan los activos que están en juego. Si conseguimos hacerlo siguiendo la estrategia correcta, conseguiremos que la operación sea mejor, más rápida, más económica y con un alto nivel de seguridad (tanto en la capacidad de evitar o reducir al máximo los tiempos no operativos o de caída de la planta como en mantener un elevado nivel de seguridad en el trabajo, con pocos incidentes o accidentes).

Ya no podemos pensar en nuestra planta de fabricación como un espacio aislado; ha de integrarse perfectamente con nuestros sistemas y dispositivos, y con los de nuestros proveedores y clientes, para disponer de una solución de fabricación inteligente y segura.

En este ámbito, podemos destacar la recomendación ISA 95 (97) de integración de sistemas de control industrial, que, partiendo de un modelo abstracto detallado de la empresa (que incluye funciones de control de fabricación, funciones de negocio y funciones de gestión de la información), establece una terminología común para la descripción y comprensión de los procesos indus-

triales (por ejemplo, para el intercambio de información entre los diferentes sistemas de información y gestión de la información, incluyendo los modelos de datos y las definiciones para todo el proceso de intercambio de información, siguiendo el conocido modelo de referencia de Purdue (98)). Siguiendo las recomendaciones, conseguiremos reducir los riesgos, los costes y los errores asociados con la implementación de los interfaces entre sistemas y dispositivos para el intercambio de información. Así, nuestro intercambio de datos será robusto, seguro y eficiente en costes.

2) Automatización de la construcción

En un entorno de alta convergencia de los sistemas de control y gestión de la fabricación, de las infraestructuras, de los servicios básicos[127] y de la edificación, es básico gestionar adecuadamente la automatización en todos los niveles. Los espacios son lo que podríamos llamar estructuras altamente complejas; por lo tanto, debemos seguir recomendaciones para tener en consideración todos los condicionantes que las afectan. Y aquí es donde radica la importancia de lo que señalamos; la complejidad no es menor por que estemos hablando del espacio de oficinas de nuestra corporación o la planta de fabricación, pues, de hecho, los diferentes sistemas de información y los diferentes dispositivos tendrán un alto nivel de interoperabilidad.

(127) En inglés se utiliza el término *utilities*.

Si pensamos en la parte de gestión de la distribución de agua en un edificio, veremos que debemos tener en consideración la provisión de agua, pero también el tratamiento del agua y, obviamente, la gestión de los desechos que de su uso se derivan; en todo momento deberemos disponer de elementos de medida y control de flujo, de nivel, de presión, de humidad, de compuestos químicos, que van a enviar un gran número de señales a válvulas y actuadores de formas muy diversas (a través de cable, comunicaciones de radio…).

Si queremos que la construcción del espacio lo dote de cierta inteligencia, deberemos disponer de soluciones que integran los sistemas de iluminación, calefacción y otros con la presencia (y cuánta) en el espacio.

Aquí, por la parte que nos ocupa en este documento, debemos además tener en consideración todos los condicionantes asociados con la seguridad, tanto en los aspectos más de seguridad física y acceso (o tránsito) del edificio como la digital (ciberseguridad).

Evidentemente, debemos tener claro que no es suficiente con disponer de los elementos de control, monitorización, gestión y alarma pertinentes para hacer frente a los problemas de seguridad que puedan surgir. Debemos, además, disponer de las herramientas de toma de decisiones y sobre todo de los procesos definidos (en nuestro plan de actuación) para saber qué hacer en todo momento y ante toda situación, y debe disponerse del personal adecuadamente cualificado y formado.

3) Comunicaciones

En un entorno altamente interconectado como una planta de fabricación, las comunicaciones están omnipresentes. Debemos ser capaces de entender las diferencias de requerimiento entre los entornos industriales, de oficina, o domésticos desde la perspectiva de las comunicaciones y las redes (de comunicación). Si añadimos la variable de seguridad (ciberseguridad), es aún más importante que seamos capaces de visualizar y caracterizar las diferencias entre los equipos de interconexión (por ejemplo, *routers*) en dichos entornos, o las prestaciones que le pedimos a un equipo de seguridad perimetral.

Desde la perspectiva de los estándares de ISA, tenemos muchos tipos de redes que nos pueden interesar: las soluciones estándares wifi (IEEE 802.11) (99), soluciones no cableadas para entornos automatizados (100), WirelessHART, Zigbee (101), las soluciones cableadas (que nos dan un nivel de garantía y seguridad más elevado, siguiendo, por ejemplo, la recomendación de compatibilidad electromagnética en instrumentación ISA50 (102)), como Ethernet Industrial (103), Profibus/Profinet (104), Ethercat (105), Anybus (106) o Modbus (107).

Es importante que entendamos que, independientemente del ámbito de operación en el que nos encontremos, las comunicaciones siempre están ahí, tanto si trabajamos con un sistema SCADA[128] o un sistema de control distribuido[129] o con «simples» controladores programables[130].

(128) *supervisory control and data acquisition* (SCADA).

(129) *distributed control system* (DCS).

(130) *programmable logic controller* (PLC).

Por último, ISA dispone recomendaciones que podríamos llamar transversales en el ámbito de las comunicaciones (108) (109) (110), que deben tenerse en consideración cuando estamos en un entorno de planta de fabricación.

4) Sistemas de control

No podemos plantearnos ningún entorno de fabricación sin sistemas de control. Evidentemente, en este ámbito tan amplio, por un lado, tenemos todos los aspectos relacionados con la teoría de control (industrial), tanto en entornos de control continuo como en control discreto. En este marco, la recomendación de control en segundo plano debe ser referente de consulta (108).

5) Ciberseguridad

(131) Del inglés, *confidentiality, integrity and availability* (CIA).

Para el ámbito que nos ocupa, sin duda este es el aspecto más importante, aun cuando los aspectos genéricos de seguridad podemos entenderlos de aplicación general. Aquí vamos a hacer hincapié en una importante diferencia en cuanto al enfoque de la ciberseguridad cuando estamos en una planta de fabricación. Los tres pilares de la seguridad son la confidencialidad, la integridad

y la disponibilidad[131]; pues bien, cuando estamos fabricando, el primer foco es la disponibilidad, por encima, por ejemplo, de la confidencialidad. La planta de fabricación tiene que estar, en primer lugar, operativa.

En el entorno de ISA, a través del su instituto de seguridad (111), se puede obtener una certificación de ciberseguridad para sistemas de control y automatización industrial, bajo el nombre de garantía de seguridad de sistemas (112), que estará asociada con la parte de seguridad de la norma IEC-62443-3-3 (que veremos más adelante).

6) Energía

En todo entorno de fabricación, el control de la energía es clave. De hecho, tanta es la importancia que las primeras fuentes en torno a *smart grids* las encontramos en documentos de la ISA. Evidentemente, tendremos que estar atentos a las fuentes de energía (fósiles o naturales) y a sus sistemas de distribución, pero también al impacto que entornos de despliegue masivo de dispositivos (*internet of things*) tienen desde el punto de vista del consumo y distribución de energía. La división de industrias de energía (113) de la ISA es un lugar de obligada revisión cuando hablamos de energía.

7) Dispositivos de control y medida y técnicas

Los aspectos relacionados con la instrumentación[132] están en el centro de las recomendaciones y estándares con los que trabaja la ISA. Tanto desde el punto de vista de las técnicas de los dispositivos de control como en la forma en la que se puede llevar a cabo la medida de la propiedad a controlar.

(132)Recordemos que originariamente la ISA era la Instrument Society of America (ISA).

8) Mantenimiento de planta y operaciones

En la operación de las plantas de fabricación debemos gestionar de forma eficiente la operación; para ello, debemos llevar un control continuado de su capacidad y de la productividad que se obtiene, estar atentos a la calidad del producto que se produce, pero no podemos descuidar la seguridad de las personas que están en planta, procurando que los tiempos de inactividad en la planta sean los menores posibles. Vamos a trabajar para prevenir los fallos catastróficos antes de que ocurran, predecir las necesidades futuras en aspectos de mantenimiento, mejorar la disponibilidad y confiabilidad de los sistemas de automatización en planta (tanto de máquinas como de procesos), implantar programas (actualizados y de referencia) para la gestión del mantenimiento de la planta, que van a permitirnos reducir los tiempos de inspección, con lo que se mejora el rendimiento operativo de la planta de fabricación (reduciendo costes y aumentando la seguridad).

9) Seguridad

Como ya hemos indicado, la seguridad en la planta es uno de los puntos críticos (ahora no estamos hablando de ciberseguridad). La norma de referencia para la seguridad de procesos (114) pasó a ser un estándar IEC 61508 (115) y IEC 61511 (116).

Con ellas vamos a poder gestionar la seguridad, en los procesos, en la planta de fabricación, pero también con los dispositivos y maquinaria.

Desde un punto de vista práctico, es importante tener a mano estudios (que nos aportan las normas) sobre riesgos y operaciones[133].

(133)En inglés se suele usar el término HAZOPs, de *hazard and operations*.

10) Símbolos, terminología y documentación

Por último, como en todos los ámbitos de trabajo, la simbología y la terminología son necesarias para la colaboración entre todos.

De todos estos ámbitos, el que nos interesa especialmente en este documento es el que hace referencia a la ciberseguridad. En este punto se definió la recomendación asociada de seguridad de sistemas de control y automatización industrial (117), para poder tener en sus comités de discusión y trabajo personal experto en el ámbito de la ciberseguridad, pero también de los diferentes ámbitos de fabricación que hemos indicado anteriormente que se trabajan en el seno de la ISA.

El objetivo principal fue trabajar para resolver (o mejorar) aquellas situaciones que impliquen la seguridad de las personas (usuarios o trabajadores), la pérdida de confianza por parte de los usuarios finales, la violación de los requerimientos normativos, la pérdida (vulnerabilidad) de la privacidad de la información, y como punto global que puedan afectar a la seguridad nacional. Obviamente, aquí se abarca cualquier tipo de planta de fabricación, cualquier infraestructura de producción, cualquier industria y cualquier sistema. En el marco de la norma, se enumeran los posibles casos sin presentar en ningún caso una lista cerrada:

- Sistemas hardware y software tales como DCS, PLC, SCADA, redes de sensores y/o sistemas de diagnóstico y monitorización.

- Personas, redes y dispositivos utilizados (interna o externamente) para facilitar y proveer los elementos de control, seguridad y gestión de las operaciones de fabricación (tanto de forma continuada como de forma intermitente, en primer plano o en segundo plano, de forma individualizada o de forma conjunta con otros procesos).

La seguridad física, que es muy importante en toda planta de fabricación, no tiene un gran énfasis en los documentos de los estándares que nos ocupan.

Es a partir de estos trabajos originales que se definirá posteriormente la norma IEC-62443, que vamos a analizar a continuación; como modelo de referencia (estándar) se define desde una perspectiva internacional y neutra (no dependiente de vendedor o fabricante), está siendo la guía de referencia, por encima de otras normas más particulares, como podrían ser la WIB-M-2784 (118) o la NERC-CIP[134] (119).

(134)NERC-CIP de North American Electric Reliability Corporation, Critical Infrastructure Protection.

3.2. Estructura de la IEC 62443

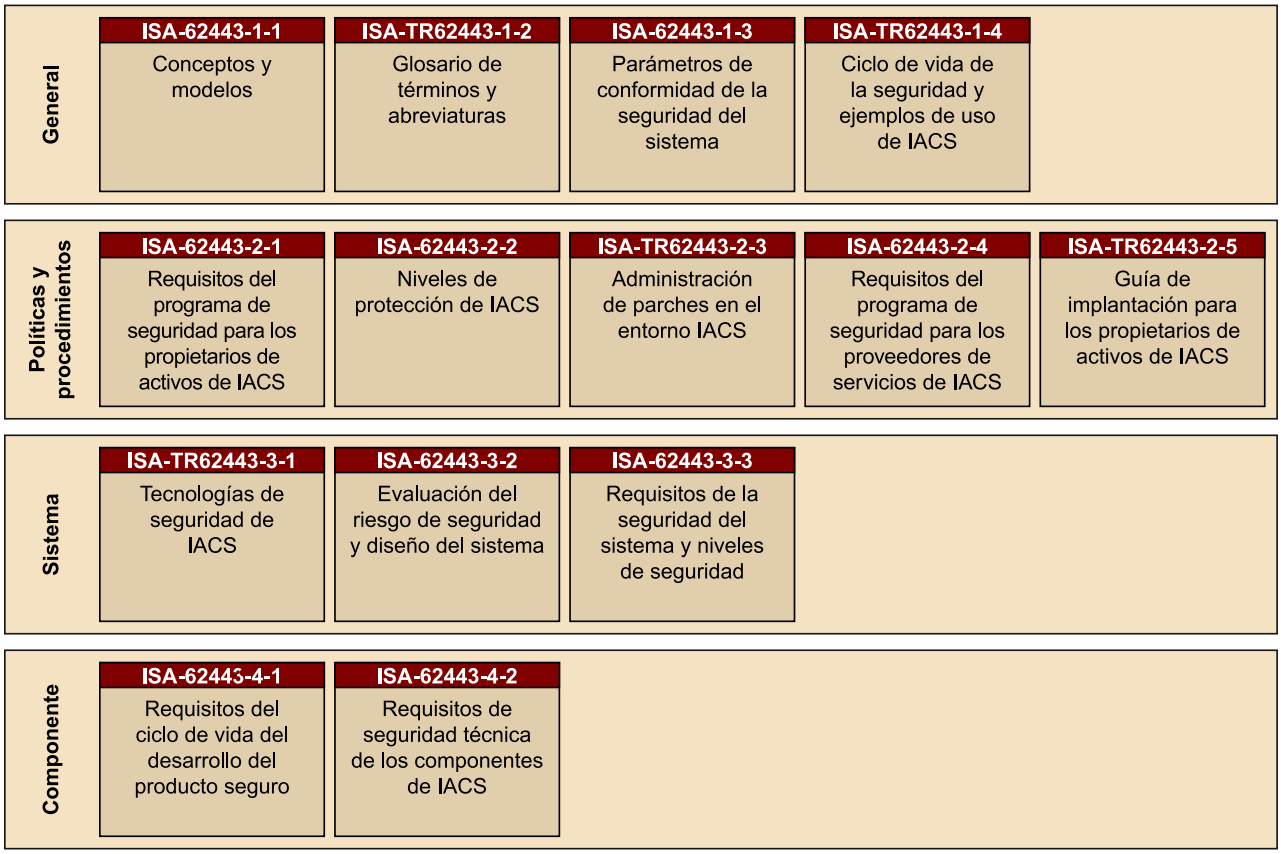
La serie de estándares de la norma 62443 se ha trabajado de forma conjunta por parte del comité ISA99 y el grupo 10 del comité técnico 65 de la IEC (120), para poder resolver de forma satisfactoria todos los aspectos relacionados con el diseño robusto y resiliente de la ciberseguridad en los sistemas de control y automatización industrial[135].

(135)En inglés IACS, *industrial automation control systems*.

En función de la referencia que sigamos, se modifica ligeramente la notación. En el caso de la ISA, la numeración es ISA-62443-x-y, y, en el caso de IEC, la numeración es IEC-62443-x-y. Ambos documentos procuran ser actualizaciones síncronas, si bien la propia diferencia en la numeración nos indica que puede haber diferencias (menores) entre ambos.

En la figura 36 (117) podemos ver el esquema general de la recomendación (desde la visión de la ISA).

Figura 36. Esquema general de la ISA-62443



Como vemos, se estructura en cuatro categorías que vamos a tratar a continuación en sus respectivos cuatro apartados, con las que vamos a garantizar, primero, la uniformidad en cuanto a conceptos relacionados con la gestión de los riesgos y amenazas, y todo el proceso de la securización (en el desarrollo, integración y operación) y la concreción en las configuraciones en el ámbito de las políticas y sistemas para una solución.

Como no puede ser de otra forma, la norma de la serie ISA/IEC 62443 se apoya en las normas de seguridad de los sistemas de información (como pueden ser las series ISO/IEC 27000), pero identificando y gestionando las particularidades propias de los sistemas de control y automatización industrial. Por ejemplo, todos los importantes condicionantes relacionados con la seguridad (de los operarios y de los consumidores) y el entorno (medio ambiente), que quizás sean menos relevantes en los entornos de seguridad de los sistemas de información.

La evolución de los diferentes documentos de la norma ISA 99/IEC 62443 sigue el siguiente esquema (121):

- ANSI/ISA-99.01.01-2007 «Security for Industrial Automation and Control Systems: Concepts, Terminology and Models». Primer documento de la serie. Se encarga de sentar las bases a usar en el resto de la serie.

- ANSI/ISA-TR99.01.02-2007 «Security Technologies for Manufacturing and Control Systems». Informe técnico publicado después del primer documento y que nació con la intención de ser revisado periódicamente para recoger las novedades del mercado. Contiene diversas herramientas de seguridad, con una descripción de su implantación y configuración en los sistemas de control industrial.

- ANSI/ISA-99.02.01-2009 «Establishing an Industrial Automation and Control Systems Security Program». Fue el último que se publicó de la serie ISA99. Describe los elementos necesarios para implantar un sistema de gestión de la ciberseguridad y proporciona una guía para conocer los requerimientos de cada uno de los elementos que lo componen.

- ANSI/ISA-99.02.02 «Operating an industrial automation and control system security program». Llegó a estar en fase de desarrollo, pero nunca se publicó ningún borrador del mismo. Su objetivo se fijaba en la operación del programa de seguridad después de su diseño e implementación. La operación incluía aspectos como la definición de métricas para cuantificar la efectividad del programa.

- ANSI/ISA–99.03.xx «Technical security requirements for industrial automation and control systems». No llegó nunca a comenzar su desarrollo. Los contenidos teóricos de esta parte del estándar incluían la definición de las características de los sistemas de control y automatización industrial que los diferencian de los sistemas de tecnologías de la información desde el punto de vista de la seguridad, definiendo requerimientos de seguridad únicos para estos sistemas.

Desde el punto de vista de la evolución temporal, las publicaciones han seguido el siguiente calendario:

- 2007: ANSI/ISA 99-1-1, ANSI/ISA-TR99-1-2.

- 2009: ANSI/ISA-99-2-1, IEC-62443-1-1, IEC-TR62443-3-1.

- 2010: IEC-62443-2-1.

- 2013: IEC-62443-3-3.

- 2015: IEC-TR62443-2-3, IEC-62443-2-4.

Formalmente, la numeración ISA99 pasa a denominarse ANSI/ISA-62443 en 2010, y se concluye la evolución de los cuatro documentos y del informe técnico iniciales a los actuales ocho documentos y cinco informes técnicos de la norma IEC/ISA 62443.

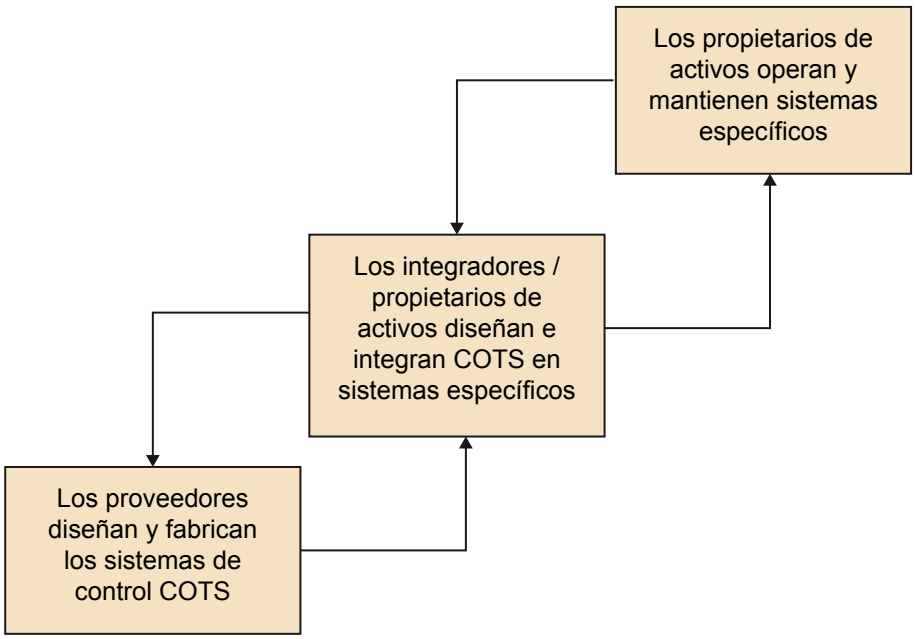
En la figura 37 (122) podemos ver cómo, en todo el proceso de gestión de la ciberseguridad en la norma IEC/ISA 62443, tenemos continuamente una interrelación entre tres agentes:

- Los propietarios de los activos (sistemas de control y automatización industrial), que suelen ser los que llevarán a cabo la operación y mantenimiento de los mismos.

- Los integradores de componentes y sistemas que llevarán a cabo su integración en los anteriores sistemas.

- Y los proveedores de sistemas y componentes, que, con la colaboración de los integradores, podrán dar respuesta a las necesidades de diseño y funcionales de nuestros sistemas de control y automatización industrial.

Figura 37. Agentes implicados en el ciclo de vida de la gestión de la ciberseguridad en la IEC/ISA 62443

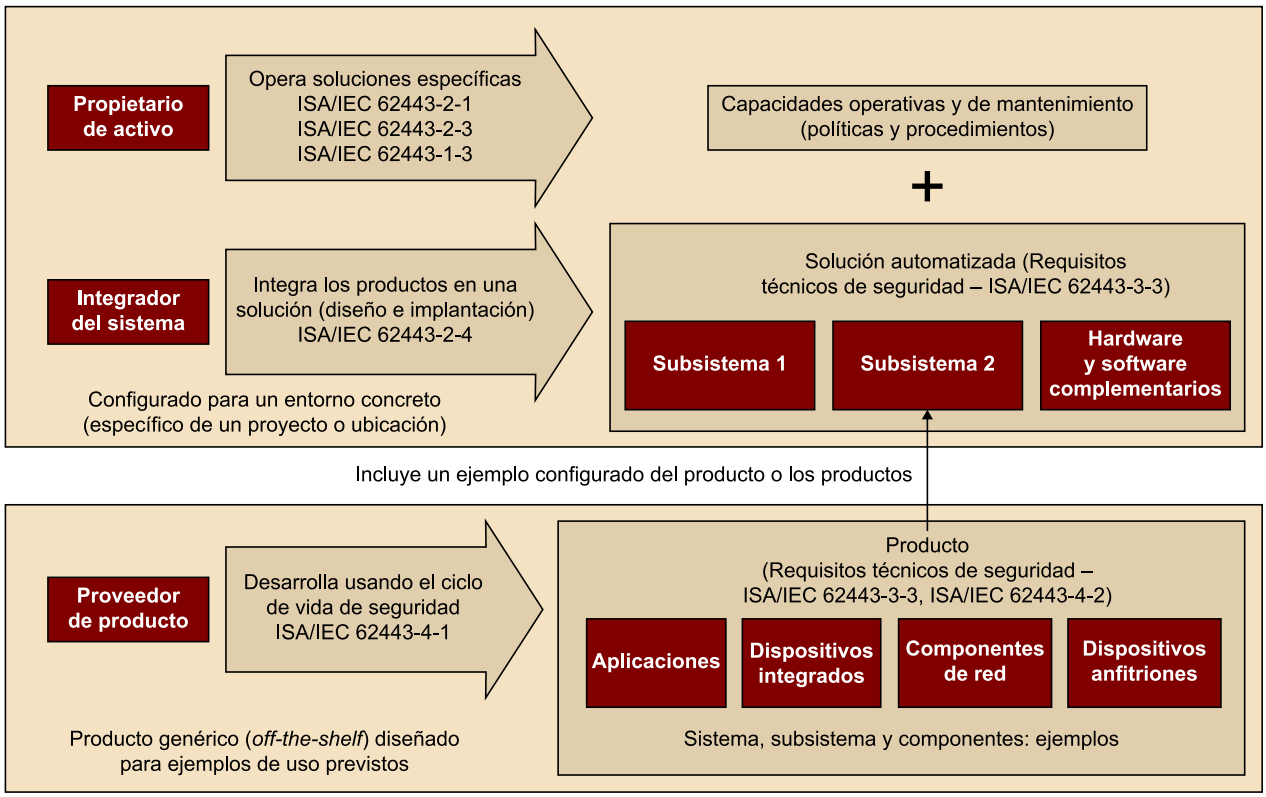


Para que el despliegue de la solución final sea satisfactorio para todos, cada uno de los agentes debe llevar a cabo su labor de forma adecuada. Por un lado, los proveedores deben garantizar que sus soluciones y componentes cumplan con los requerimientos que les demandaremos, tanto desde la perspectiva de seguridad como en la de las prestaciones de rendimiento[136]. Por otro lado, los integradores deben garantizar que utilizan las (buenas) prácticas necesarias para asegurar que la puesta en marcha de la solución mantiene los requerimientos de seguridad en todos sus condicionantes (personas, entorno, producto…). Por último, los propietarios de los activos deben seguir las guías de operación y mantenimiento del sistema desplegado, para mantener en todo momento los condicionantes de ciberseguridad que durante el ciclo de diseño y puesta en marcha se han definido, y evitar que a lo largo de la vida útil del sistema se vayan degradando sus niveles de ciberseguridad.

[136]Cuando se habla de diseño por parte de un proveedor de una solución o sistema que debe dar respuesta a demandas del mercado, se utiliza el término COTS, del inglés *commercial-off-the-shelf*.

Como vemos, el proceso, además de ser continuado, debe poder asegurar que todas las piezas del rompecabezas cumplen con su responsabilidad, por lo que la norma se descompondrá en diferentes categorías que van a hacer énfasis en cada uno de los agentes de la cadena de valor. Ved la figura 38 (123).

Figura 38. Relación de los diferentes componentes de la norma IEC/ISA 62443 con proveedores, integradores y propietarios de los sistemas de control y automatización industrial



3.2.1. Categoría general

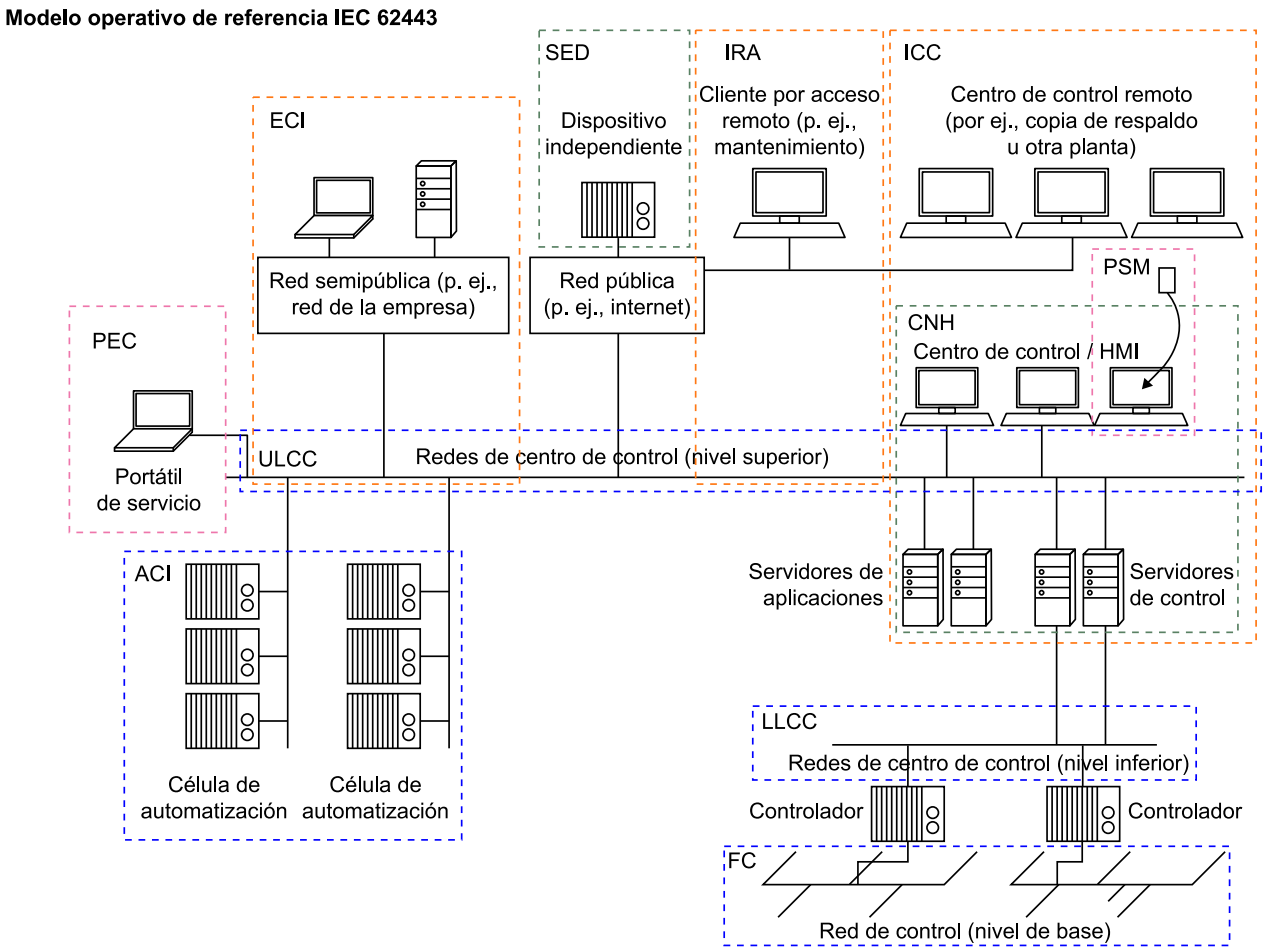
Abarca cuatro recomendaciones:

1) ISA-62443-1-1, de conceptos y modelos (124)

Se describen los conceptos básicos y modelos referidos a la ciberseguridad en los entornos industriales.

En este sentido, se trabaja sobre un modelo de referencia como el de la figura 39 (125).

Figura 39. Modelo de referencia para IEC/ISA 62443



Aprovechando el esquema, parte del vocabulario que se define aquí responde a los acrónimos que ponemos a continuación (en inglés directamente, para que tengan su correspondencia más clara).

ECI, External Network - Control Network Interconnection.

IRA, Interactive Remote Access to a Control Network.

ICC, Inter-Control Center Access to a Shared Control Network.

SED, Standalone Embedded Device.

PEC, Portable Engineering Computer.

PSM, Portable Storage Medium.

ACI, Inter-Area Communication within a hierarchical multi-area Control Network.

CCN, Control Center Networks within a single Control area.

FCN, Field Control Networks within a single Control Area.

CNH, Control Network Host.

1AFD, Automation Field Device.

Dos de los aspectos más importantes de todas las medidas presentes a lo largo de la norma son las llamadas zonas de seguridad y los conductos[137]:

(137)En inglés, *security zones* y *conduits*.

- Las zonas de seguridad son una forma de agrupar los activos (tanto físicos, como lógicos) que, de alguna forma, comparten requerimientos de seguridad comunes. Una zona, por lo tanto, conlleva un borde (perímetro) de la zona, y por lo tanto se podrá distinguir los componentes (dispositivos, sistemas) internos y/o externos a la zona.

- Los conductos representan los caminos entre dos zonas de seguridad. Por lo tanto, va a ser aquí donde vamos a definir las políticas y procesos de seguridad entre dos zonas de seguridad. Toda comunicación entre zonas de seguridad deberá llevarse a cabo a través de conductos. Podrán definirse políticas de seguridad comunes y estándares para ser aplicadas en diferentes conductos, y/o en diferentes momentos y situaciones.

Esto es importante desde la perspectiva de la seguridad porque, al agrupar los activos y comunicarlos por caminos conocidos, es más fácil, en la mayoría de las ocasiones, poner medidas de seguridad para asegurar los conductos que asegurar cada uno de los activos de manera independiente.

2) ISA-TR62443-1-2, de glosario maestro de términos y abreviaciones

En este documento (informe técnico) se recoge un glosario de términos y las abreviaturas usadas en la serie.

3) ISA-62443-1-3, de métricas de conformidad de la seguridad de sistemas

En este documento, se presenta un conjunto de métricas cuantitativas postuladas sobre la base de los requerimientos tanto de sistemas como de procesos.

4) ISA-TR62443-1-4, de ciclo de vida de seguridad en entornos IACS y caso de uso

En forma de informe técnico, se hace una descripción del ciclo de vida de la seguridad en los entornos de los sistemas de control y automatización industrial. Para reforzar los conceptos, se presentan casos de uso.

El ciclo de vida de los sistemas de control y automatización industrial incluye los proveedores de sistemas y componentes, los integradores de sistemas, los propietarios y responsables de los activos, y los proveedores de servicios,

pues sin ellos el ciclo no es completo. Podríamos decir que el ciclo de vida empieza con el desarrollo de los componentes considerados como elementos individuales (como podrían ser los controladores individualizados, o en una fase mayor todos los componentes que conforman un sistema, o incluso todos los sistemas que están implicados en un proceso). Un integrador de sistemas suele ensamblar diferentes productos, componentes y sistemas en la solución final de automatización y control, que será finalmente puesta en marcha en el marco de nuestros sistemas de control y automatización industrial.

3.2.2. Categoría de políticas y procedimientos

Abarca cinco recomendaciones, que giran todas alrededor de las políticas y procedimientos asociados con la seguridad de los sistemas de control y automatización industrial.

1) ISA-62443-2-1, de requerimientos de programas de seguridad para propietarios de activos IACS

En este documento, se define la base para la definición y puesta en marcha de un sistema de gestión de la seguridad para los sistemas de control y automatización industrial. Se busca un alineamiento importante con las recomendaciones en cuanto a despliegue de sistemas de gestión de la información propios de la serie 27000.

2) ISA-62443-2-2, de niveles de protección IACS

En este documento se dan las guías para la operación efectiva de los sistemas de gestión de los sistemas de control y automatización industrial desplegados siguiendo las pautas de la recomendación anterior.

3) ISA-TR62443-2-3, de gestión de parches en entornos IACS

Este informe técnico describe las guías para la gestión de parches (y actualizaciones) en los sistemas de control y automatización industrial que están en operación.

4) ISA-62443-2-4, de requerimientos de programas de seguridad para proveedores de servicios IACS

En este documento, se dan las guías de operación de los sistemas de control y automatización industrial para las operaciones con los proveedores de los mismos.

Los primeros trabajos en esta línea de actuación se desarrollaron bajo el paraguas del grupo de trabajo 10, del comité técnico 65 de la IEC (126).

5) ISA-TR62443-2-5, de guía de implementación para propietarios de activos IACS

3.2.3. Categoría de sistema

Abarca tres recomendaciones:

1) ISA-TR62443-3-1, de tecnologías de seguridad para IACS (127)

Este informe técnico describe cómo aplicar diferentes tecnologías de seguridad en el entorno de los sistemas de control y automatización industrial. Es el espacio de referencia para poder tener presentes, en todo momento, las soluciones tecnológicas que podremos utilizar para nuestros entornos industriales.

Se describen diversas categorías de tecnologías de seguridad en el ámbito de los sistemas de control, con una enumeración de los productos en cada una de las categorías, cuáles son las ventajas e inconvenientes de cada producto en las aplicaciones de control y automatización industrial, especialmente en lo que se refiere a la gestión de vulnerabilidades y amenazas; todo ello acompañado de las necesarias guías de configuración y de puesta en marcha.

Como muestra de lo que nos podemos encontrar las categorías del documento, son:

- Tecnologías de autenticación y autorización, donde tenemos soluciones basadas en roles (perfiles), soluciones de autenticación por contraseña, soluciones de autenticación a través de mecanismos de reto[138], soluciones de autenticación a través de mecanismos de *token* físico, soluciones de autenticación a través de tarjetas inteligentes, soluciones de autenticación a través de soluciones biométricas, soluciones de autenticación basadas en la identificación de la localización, tecnologías de gestión y distribución de contraseñas, soluciones de autenticación entre dispositivos (de dispositivo a dispositivo).

(138)En inglés se utiliza el concepto de *challenge/response*.

- Tecnologías de control de acceso, donde tendremos información sobre soluciones de filtrado, bloqueo y control de acceso, entre otros, sobre cortafuegos de red, cortafuegos basados en máquina[139], soluciones de virtualización de red.

(139)En inglés *host-based firewall*.

- Tecnologías de validación de datos y encriptación, donde podremos repasar los conceptos de soluciones de encriptación de clave simétrica, los sistemas de encriptación de clave pública y los sistemas de distribución y gestión de claves (públicas) y, por lo tanto, de su aplicabilidad en las redes privadas virtuales.

- Tecnologías de monitorización, con soluciones y herramientas para las tareas de detección (de intrusiones), la monitorización de los sistemas, la medida del estado de los sistemas, la auditoría de los sistemas, y la gestión proactiva o reactiva de los sistemas y sus posibles incidentes de seguridad. Entre otros aspectos, se desarrollarán las herramientas para la gestión de registros[140], los sistemas de detección de virus y códigos maliciosos, los sistemas de detección de intrusiones (IDS), los escaneadores de vulnerabilidades, las herramientas para el análisis forense[141], las herramientas de gestión de las configuraciones de sistemas[142] y las plataformas de gestión automatizada de programas y aplicaciones[143].

- Tecnologías y aplicaciones informáticas para los sistemas de control y automatización industrial que van a permitirnos una mejor gestión de los sistemas que tenemos desplegados, desde el punto de vista, primero, de los sistemas operativos de los servidores y estaciones de trabajo que podamos tener desplegados, los (nuevos) sistemas operativos en tiempo real y las tecnologías web.

- Los controles de seguridad físicos, que hacen referencia a la protección física de las instalaciones y dispositivos, pero también a la seguridad de las personas de las que somos responsables.

Como el elemento común de todas las tecnologías que se manejan es la ciberseguridad, todas ellas se enfocarán para dar respuesta a los siguientes aspectos:

- Las vulnerabilidades de seguridad que se afrontan con la tecnología, las herramientas o las contramedidas presentadas.

- El modelo estándar de despliegue de la tecnología, herramientas, soluciones o contramedidas.

- Los puntos débiles conocidos asociados con ello.

- Las garantías para su utilización en un entorno de sistemas de control y automatización industrial como los que ocupan a la norma.

- Las directrices futuras en las que se pueda estar trabajando.

- La concreción de guías y recomendaciones para su implantación, diseño y mantenimiento.

- La lista de fuentes de referencia y material de referencia.

2) ISA-62443-3-2, de gestión de riesgos de seguridad y diseño de sistemas

(140) En inglés *logs*.

(141) En inglés se utiliza la terminología FAT, de *forensic analysis tools*.

(142) En inglés se utiliza la terminología HCM, de *host configuration management*.

(143) En inglés se utiliza la terminología ASM, de *automated software management*.

Es importante que visualicemos que, en este documento, cuando se habla de la gestión de riesgos en el ámbito de la seguridad y diseño de sistemas, no encontraremos una guía de cómo se despliegan las soluciones, sino más bien una descripción (enumeración) de aquello que debemos hacer. No es un listado del cómo, sino del qué.

Deberemos, luego, buscar el cómo en otros documentos, recomendaciones o guías. Es un conjunto de recomendaciones sobre cuáles son las medidas que deben desplegarse para la gestión de la seguridad.

Para que podamos entender el nivel de detalle, pondremos algunos ejemplos:

- Podemos encontrar, en su apartado 4.5.1.1, una entrada que nos pide que deberemos desplegar/disponer de una lista de todas las amenazas que podrían afectar a los activos en (por ejemplo) una zona concreta. Pero en ningún caso nos va a indicar cómo podemos obtener dicha lista. De hecho, la recomendación nos devolverá una lista de acciones a desplegar, pero no cómo desplegarlas.

- Podemos encontrar, en su apartado 4.5.2.1, una entrada que nos pide que deberemos identificar y a continuación documentar todas las posibles vulnerabilidades que podamos encontrarnos en una zona, pero nuevamente no nos indica cómo hacerlo.

- Podemos encontrar, en su apartado 4.6.1.1, una entrada que nos pide que deberemos calcular el riesgo residual para cada una de las amenazas identificadas en el apartado 4.5.5, lo cual deberá poder ser comparado con el nivel de riesgo tolerable de la organización (que debe ser especificado en el apartado 4.3). Deberemos poner en marcha contramedidas de seguridad adicionales si el nivel de riesgo residual supera el nivel tolerable. Sin embargo, al respecto de cómo calculamos todos estos niveles de riesgo, en la norma, no hay ni siquiera una pista.

Respecto al documento, una parte relevante es la que nos marcará que deberemos dividir nuestro entorno en diferentes zonas y conductos (canales). Una vez tengamos la división, para cada una de las diferentes zonas deberemos definir su nivel de seguridad.

Los diferentes niveles de seguridad que nos indica la norma son:

- Niveles de seguridad objetivo[144]; hace referencia a las garantías de seguridad que quisiéramos tener en el sistema.

- Niveles de seguridad de potencial[145]; hace referencia a las garantías de seguridad que, con la configuración actual, debería tener el sistema.

(144) En inglés se utiliza la terminología T-SL (SL-T) (*target security level*).

(145) En inglés se utiliza la terminología C-SL (SL-C) (*capability security level*).

- Niveles de seguridad obtenido[146]; hace referencia a las garantías de seguridad que realmente (después del despliegue) tenemos en el sistema.

(146)En inglés se utiliza la terminología A-SL (SL-A) (*achieved security level*).

La diferenciación de estos tres tipos de niveles de seguridad nos indica claramente que la seguridad deseada es una cosa, la que esperamos tener con las contramedidas que hemos puesto en marcha es otra, y por último, la realmente obtenida (que deberemos medir de alguna forma) es una tercera. La seguridad no es una ciencia exacta y el nivel potencial (esperado podría ser otra forma de definirlo) no tiene por qué ser el nivel realmente alcanzado. Es, por lo tanto, imprescindible incluir, en todos nuestros procesos, la medida de los niveles de seguridad con los que estamos trabajando, y por eso la recomendación hace énfasis en esta triple clasificación tipológica.

La recomendación no nos da demasiadas pistas sobre cómo llevar a cabo la clasificación; suele ser una buena pauta pensar en las consecuencias potenciales que un posible ataque pudiera causar en cada una de nuestras zonas.

Con el aumento del nivel de seguridad, se aumenta la complejidad de las soluciones que vamos a tener que desplegar para mitigar los posibles efectos. Para cada caso, el nivel de seguridad que definamos (como objetivo, potencial o realmente obtenido) debe hacer referencia a la zona (en global), pero una buena manera de poder obtener el nivel de seguridad de una zona parte de conocer el nivel de seguridad de cada uno de los elementos y componentes de la zona.

Conjuntamente con las definiciones de este documento, respecto a los niveles de seguridad de nuestros sistemas, tenemos también la recomendación IEC62443-4-2, que hará referencia a los niveles de seguridad de los componentes de nuestro sistema de control y automatización industrial.

Los diferentes niveles de seguridad con los que se trabaja hacen referencia a diferentes ámbitos (llamémoslos funcionales) de nuestro sistema, que detallamos a continuación:

- Requerimiento funcional 1: controles de identificación y autenticación.
- Requerimiento funcional 2: controles de uso.
- Requerimiento funcional 3: integridad del sistema.
- Requerimiento funcional 4: confidencialidad de datos.
- Requerimiento funcional 5: flujo de datos (restricción).
- Requerimiento funcional 6: tiempo de respuesta ante eventos.

- Requerimiento funcional 7: disponibilidad de recursos.

Si deseamos que un dispositivo, componente o sistema[147] esté clasificado en un determinado nivel de seguridad (por ejemplo, el 3), deberá cumplir este nivel de seguridad para los siete requerimientos funcionales enumerados anteriormente. De todas formas, se indica para cada requerimiento y nivel cuáles son las condiciones de pertenencia, y, por lo tanto, si conocemos las condiciones de funcionamiento de nuestro sistema, podremos entender cuáles son los requerimientos funcionales que tendremos que cumplir en cada uno de los ámbitos.

[147]Las indicaciones respecto a los requerimientos de seguridad de los sistemas de esta norma serán similares en el caso de la norma de requerimientos de seguridad de los componentes de los sistemas de control y automatización industrial.

3) ISA-62443-3-3, de requerimientos de seguridad de sistemas y niveles de seguridad (128) (129)

Este documento nos detallará los requerimientos técnicos de nuestros sistemas de control, en relación con cada uno de los siete requerimientos funcionales que se describen en la norma IEC-62443-1-1 y que también hemos referido en el apartado de la norma IEC-62443-3-2.

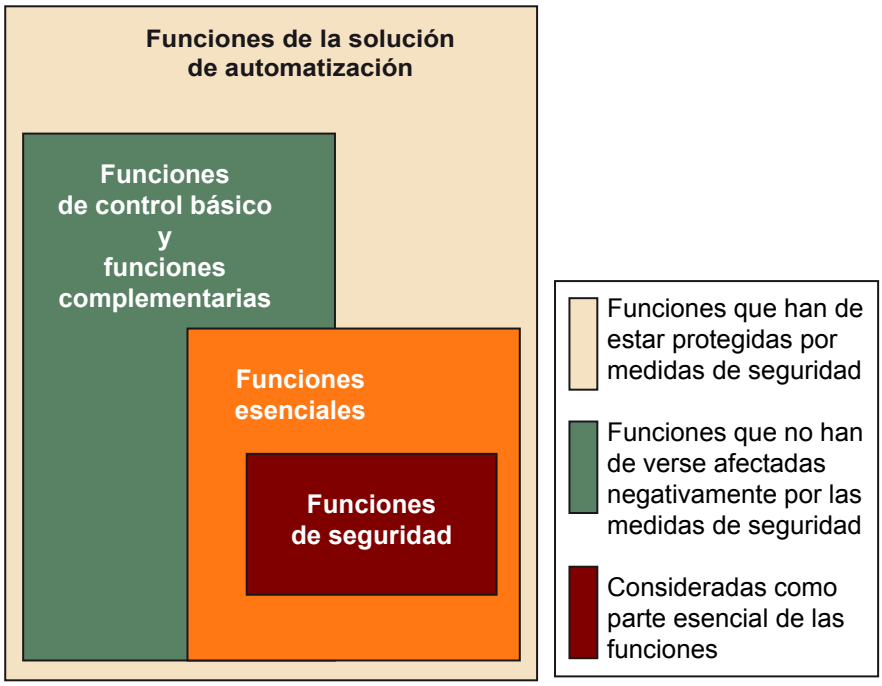
En este punto, la norma define las funciones esenciales como aquel proceso, función, funcionalidad, componente, elemento o dispositivo que es necesario e imprescindible en nuestro entorno para garantizar y mantener la seguridad, el entorno y la disponibilidad de nuestro sistema.

Como vemos en la figura 40 (130), podemos clasificar las funciones de nuestro sistema de control y automatización industrial como:

- Funciones esenciales (que no deberán nunca verse negativamente afectadas por nuestras medidas de seguridad), que englobarán las funciones de seguridad.

- Funciones de control básico y funciones complementarias, que deberemos proteger por nuestras medidas de seguridad.

Figura 40. Tipos de funciones de los sistemas de control y automatización industrial



Cuando estamos trabajando con niveles de seguridad de nuestro sistema, es relevante que tengamos en cuenta la importancia que tiene el proceso de documentación y definición de cualquier proceso.

A este respecto, la recomendación nos habla de cuatro niveles de madurez de la definición (del documento, del proceso, de la configuración del sistema...):

- Nivel de madurez 1: proceso a medida.
- Nivel de madurez 2: proceso documentado, pero que puede no ser fácil repetir.
- Nivel de madurez 3: proceso documentado, que podríamos repetir de forma consistente en diversas situaciones.
- Nivel de madurez 4: proceso documentado, que podríamos repetir de forma consistente en diversas situaciones, y qué podríamos mejorar.

Para la recomendación, los niveles de madurez no tienen relación alguna con los niveles de seguridad, por lo que son dos clasificaciones independientes la una de la otra. En realidad, si deseamos aumentar los niveles de seguridad, es importante que los niveles de madurez sean lo mayor posible, pues la mejor manera de poder aumentar nuestros niveles de seguridad es documentar de forma adecuada nuestros procesos.

3.2.4. Categoría de componentes

Abarca dos recomendaciones de reciente aparición (131):

1) ISA-62443-4-1, de requerimientos para el ciclo de vida de desarrollo de producto seguro (132)

Este documento define los requerimientos de todos los procesos implicados en el desarrollo seguro de los productos usados en los sistemas de control y automatización industrial. Toda la teoría conocida sobre el desarrollo seguro de productos[148], tanto desde el punto de vista del desarrollo como desde las visiones de las recomendaciones en ciberseguridad. Desplegaremos un conjunto de guías para garantizar cada una de las fases del desarrollo de producto. Desde su diseño hasta el final de su vida útil, hemos de ser capaces de garantizar los requerimientos de seguridad del sistema.

(148)En inglés utilizamos la terminología SDL *secure development life-cycle*.

Cuando pensamos en el ciclo de vida, de un proceso de desarrollo, hemos de considerar todos los elementos que le afectan:

- La concreción de los requerimientos de seguridad.
- La definición que de ellos se deriva.
- La implementación, que debe incluir obviamente guías de codificación (segura).
- Los mecanismos definidos y en operación para la verificación y validación de la solución.
- La gestión de los posibles defectos que se puedan producir en el producto y las acciones que de ellos se deban derivar.
- La gestión de los parches y las actualizaciones, en el momento de la operación y utilización del desarrollo.
- Los mecanismos asociados con el fin de vida del producto.

Como el documento hace referencia al desarrollo de producto, no son recomendaciones que deban ser consideradas (en principio, pese a que siempre hay que tener una mirada amplia de las afectaciones laterales a nuestras propias responsabilidades) por parte de los integradores de los sistemas. Es un documento dirigido a los desarrolladores del producto, a los que puedan operar el producto (en la afectación de las guías de actualización, por ejemplo), pero no a los integradores del producto.

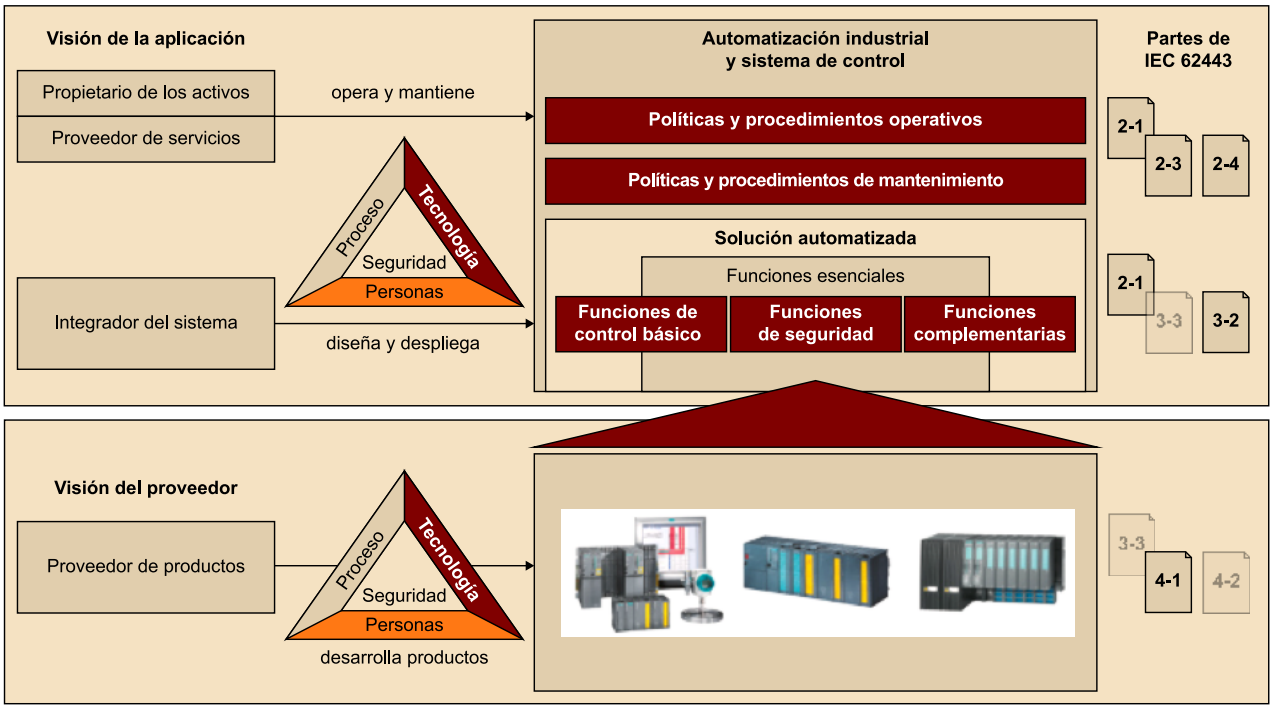
2) ISA-62443-4-2, de requerimientos técnicos de seguridad para componentes IACS (133)

Este documento que es muy fresco, dará las pautas técnicas de seguridad para propietarios de activos, integradores de sistemas, proveedores de productos, e incluso para las agencias de normalización y auditoría, referentes a los componentes de los sistemas de control y automatización industrial, haciendo especial énfasis en los componentes integrados, los elementos de interconexión, los sistemas y las aplicaciones.

El objetivo es disponer de las guías para habilitar las funcionalidades que aumenten el nivel de seguridad de todos los elementos de nuestros procesos, que nos permitan mitigar las amenazas hasta un determinado nivel, sin tener que desplegar *a posteriori* contramedidas que compensen los daños sufridos.

En la figura 41 (130), podemos ver los diferentes agentes que participan en la norma IEC 62443.

Figura 41. Agentes que participan de la seguridad en los sistemas de control y automatización industrial



3.3. *Conformity assessment program*

Con la estructuración de la norma IEC 62443, tenemos una serie de guías y recomendaciones que nos han de permitir desplegar, de forma segura, las herramientas y soluciones para aumentar el nivel de seguridad de nuestros sistemas de control y automatización industrial.

En este sentido, el programa de evaluación de nuestro grado de cumplimiento de la norma[149] define un conjunto de actividades diseñadas para validar (certificar) que un producto o servicio cumple con los requerimientos establecidos, en nuestro caso, en la norma IEC-62443.

[149]En inglés se utiliza la terminología *conformity assessment program*.

Por un lado, tenemos la descripción técnica de los requerimientos que debe cumplirse a nivel de seguridad, y si pasamos la certificación el producto podrá visualizar su sello de cumplimiento normativo.

Los mecanismos de evaluación de la conformidad de cumplimiento de requerimientos, en un mundo cada vez más complejo y entrelazado, van a permitir a todos los eslabones de la cadena de valor apoyarse en las soluciones y productos de terceros para sus propios desarrollos, o para el diseño, puesta en marcha y mantenimiento de cualquier nuevo proceso y sistema.

Para cada norma que podamos tener, pues tendremos definidos los mecanismos para la certificación del cumplimiento de la norma.

En el caso de la ISA (134), solo ha sido recientemente cuando se ha visto la necesidad de dotar de un programa de certificación para la gran cantidad de estándares que se habían estado desarrollando durante años. Ha sido a partir de ese momento que se ha puesto en funcionamiento una unidad para la puesta en marcha (definición) y posterior ejecución de las operaciones de certificación. Esta unidad es el Instituto de Certificación de Seguridad de la ISA (135).

En el seno de la ISA se despliegan dos programas de certificación que se apoyan en soluciones y plataformas de certificación de terceros, que acreditan que un producto es seguro y cumple con los requerimientos que de él se esperan en términos de rendimiento, seguridad u otros criterios que podamos incluir en el programa de certificación.

En el caso que nos ocupa, uno de los dos programas de certificación es el programa de certificación de ciberseguridad ISASecure® que nos certificará el cumplimiento de los requerimientos de seguridad de la ISA/IEC 62443. El segundo de los programas certifica sensores para soluciones no cableadas y dispositivos acordes con la norma ISA 100.11a-2011 o IEC 62734, en el seno del instituto para compatibilidad no cableada ISA100 (136).

El conjunto de certificaciones, en el marco de ISASecure (112), se ha ido incrementado en estos últimos años.

En el marco de interés para nosotros, en lo que haga referencia a la norma IEC/ISA 62443, la primera certificación data del 2014, en relación con el documento (apartado) 62443-3-3. Es la certificación en seguridad de sistemas, que permite evaluar los productos de control y automatización industrial (comerciales).

Se llevó a cabo una revisión del proceso de certificación en julio de 2016 (versión 2.0), que ya debía seguirse en todos los procesos de certificación en lo que hace referencia a los proveedores, los integradores o propietarios y gestores de los activos finales (sistemas y dispositivos finales de control y automatización industrial).

Como ejemplo del proceso de certificación, se incluye un proceso de test de vulnerabilidades utilizando la herramienta Nessus (137) y una base de datos de vulnerabilidades como referencia (138). También se añadieron procedimientos de mejora de los test de robustez en las comunicaciones, y en la fase de validación de los requerimientos del ciclo de vida del desarrollo de producto.

En este mismo sentido de mejora y ampliación del proceso de certificación, el ISCI[150] publicó en 2014 (139) una versión del proceso para la certificación del ciclo de vida del desarrollo de soluciones de control y automatización industrial (en modalidad independiente[151]), que se alineará con la norma ISA/IEC 62443-4-1.

(150) ISA Security Compliance Institute.

(151) En inglés se utiliza el término *stand-alone*.

4. Evaluación de la seguridad

4.1. Servicios de alerta (CERT-SI)

A principios de la década de los noventa, surge en Europa, a semejanza de las iniciativas en Estados Unidos (el primero en Carnegie Mellon University (140)), la necesidad de crear equipos de respuestas a incidentes de seguridad en ordenadores[152]. Su función principal (entonces y así sigue a grandes rasgos) es la de:

[152]El término CERT se refiere a coordinación de emergencias en redes telemáticas.

- Informar sobre vulnerabilidades de seguridad y amenazas.
- Divulgar y poner a disposición de la comunidad información que permita prevenir y resolver incidentes de seguridad.
- Realizar investigaciones relacionadas con la seguridad informática.
- Educar a la comunidad en general sobre temas de seguridad.

La creación de la capacidad de respuesta a incidentes, CCN-CERT (141), en el año 2006, y del Organismo de Certificación (142) (OC), en 2007, es la respuesta más importante al desafío planteado en su momento por parte del Gobierno de España.

La creación del CCN-CERT vino a suplir la ausencia de un CERT gubernamental/nacional en España, a imagen y semejanza de los existentes en todos los países de nuestro entorno, justo en un momento en el que este tipo de equipos se vieron como una de las mejores respuestas a los problemas de ciberseguridad. De hecho, el primer CERT (Computer Emergency Response Team) fue creado por el Departamento de Defensa norteamericano y la Universidad Carnegie Mellon (que tiene registrado el término), en Estados Unidos, en 1988. En España, el primer equipo de estas características fue el creado por la Universidad Politécnica de Cataluña (143) (esCERT-UPC), al que siguieron otros, tanto públicos como privados.

Con la puesta en marcha del Centro Criptológico Nacional se impulsó, por un lado, la constitución de un organismo para la certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que pudiera ser de aplicación a productos y sistemas de ámbito diverso. Dicho Organismo de Certificación quedó articulado en base al Reglamento de evaluación y certificación de la seguridad de las tecnologías de la información (144).

Por otro lado, se potenció el CERT Gubernamental Nacional para acabar desplegando el Esquema Nacional de Seguridad (ENS) (145), estructurado en un conjunto de 75 medidas de seguridad, que tenemos representadas en la figura 42 (146).

Figura 42. Medidas de seguridad recogidas en el Esquema Nacional de Seguridad

4.1.1. El Sistema de Seguridad Nacional (DSN)

En el marco de la Estrategia de Seguridad Nacional, se describen los riesgos y amenazas que pueden afectar de forma singular a la seguridad nacional, así como los factores potenciadores que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos. Se podría enumerar de la siguiente forma (147):

- Conflictos armados, que siguen representando una amenaza capital para la seguridad.

- Terrorismo, como amenaza directa a la vida y la seguridad de las ciudades, sobre todo afectando a intereses vitales y estratégicos, infraestructuras, suministros y servicios críticos.

- Ciberamenazas, que se despliegan en un ámbito en el que se han diluido las fronteras, permitiendo una globalización sin precedentes que propicia nuevas oportunidades pero conlleva enormes riesgos y amenazas. La dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. Los ciberataques, ya sean en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo, se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas. El bajo coste y mínimo riesgo que

suponen para el atacante y su fácil empleo, efectividad y accesibilidad son factores que explican la extensión del fenómeno.

- Crimen organizado, caracterizado por su naturaleza transnacional, opacidad, flexibilidad, capacidad de adaptación y de recuperación, así como por su movilidad.

- Inestabilidad económica y financiera, considerada uno de los principales riesgos actuales, no solo por la conflictividad política y social que genera, sino también porque alimenta y refuerza otros riesgos existentes.

- Vulnerabilidad energética, donde existe (en el caso de España es claro) muchas veces una excesiva dependencia del exterior para el abastecimiento energético. Esta vulnerabilidad de baja interconexión energética se acrecienta en un nuevo contexto geoestratégico caracterizado por el rápido crecimiento económico de grandes países, que se traduce en un gran incremento de la demanda de energía, desatando una competencia creciente por unos recursos escasos, que podría sacar del marco del mercado y derivar en conflictos por el control de los recursos energéticos.

- Proliferación de armas de destrucción masiva (nucleares, químicas y biológicas) y de sus sistemas de lanzamiento (misiles balísticos y de crucero) que deriva en una grave amenaza de seguridad nacional.

- Flujos migratorios irregulares que, aunque han tenido lugar en todos los momentos históricos, las dinámicas que han experimentado en las últimas décadas, así como su volumen los ha transformado en un fenómeno con implicaciones en la política de seguridad nacional.

- Espionaje, que se ha adaptado al nuevo escenario del mundo globalizado y aprovecha ahora las posibilidades que ofrece el ciberespacio. Las agresiones por parte de estados, grupos o individuos con la finalidad de lograr información que les permita obtener ventajas estratégicas políticas o económicas son una constante y una amenaza de primer orden para la seguridad nacional (148).

- Emergencias y catástrofes naturales, que, aunque siempre han estado ahí, últimamente su impacto es mucho mayor, por los activos que pueden perderse ante una catástrofe, y porque, en algunos casos, podrían derivarse de una acción controlada e intencionada (¿podemos provocar situaciones de catástrofe natural, para provocar un incidente de seguridad, y que no se pueda saber el origen del ciberataque?).

- Vulnerabilidad del espacio marítimo, que *a priori* nos parecería que no debe ser de importancia en aspectos de seguridad nacional, cuando pensamos que (1) dos terceras partes del planeta es espacio marítimo, y (2) la protección del mismo es muy débil: no tenemos los controles del espacio

aéreo, no tenemos un marco regulador tan claro al respecto, y por lo tanto, es un espacio idóneo para la propagación relativamente simple de riesgos y amenazas a la seguridad nacional.

- Vulnerabilidad de las infraestructuras críticas y servicios esenciales de gran impacto en la sociedad actual, por la complejidad de los sistemas de provisión de servicios esenciales. Dichos servicios son fundamentales para la seguridad de los ciudadanos, pero también para su bienestar social y económico, su salud o el mantenimiento de las funciones sociales básicas, o para un adecuado funcionamiento de las instituciones del Estado.

Evidentemente, desde la perspectiva de la respuesta a estos riesgos, se plantea una línea de actuación para cada uno de ellos (147):

- Defensa nacional: hacer frente a los conflictos armados que se puedan producir como consecuencia tanto de la defensa de los intereses o valores exclusivamente nacionales, en los que se intervendría de manera individual, como de la defensa de intereses y valores compartidos en virtud de nuestra pertenencia a organizaciones internacionales tales como la ONU, la OTAN o la UE, en los que se intervendría conforme a sus tratados constitutivos junto con otros aliados o socios.

- Lucha contra el terrorismo: neutralizar la amenaza que representa el terrorismo y reducir la vulnerabilidad de la sociedad ante sus ataques, haciendo frente a los procesos de radicalización que lo puedan preceder o sustentar.

- Ciberseguridad: garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.

- Lucha contra el crimen organizado: impedir el asentamiento de los grupos criminales organizados, poner a disposición de la justicia a los que ya operan dentro de nuestras fronteras e impedir la consolidación de sus formas de actuación delincuencial.

- Seguridad económica y financiera: potenciar un modelo de crecimiento económico sostenible, mitigar los desequilibrios de los mercados, luchar contra las actividades delictivas, potenciar la presencia económica internacional de España y garantizar la resiliencia de los servicios esenciales económicos y financieros.

- Seguridad energética: diversificar las fuentes de energía, garantizar la seguridad del transporte y el abastecimiento e impulsar la sostenibilidad energética.

- No proliferación de armas de destrucción masiva: impedir la proliferación, evitar el acceso a sustancias peligrosas por parte de terroristas o criminales y proteger a la población.

- Ordenación de flujos migratorios: prevenir, controlar y ordenar los flujos migratorios irregulares en nuestras fronteras que constituyen, a su vez, límites exteriores de la UE.

- Contrainteligencia: adoptar medidas de contrainteligencia en la defensa de los intereses estratégicos, políticos y económicos de España, para prevenir, detectar y neutralizar las agresiones encubiertas procedentes de otros estados, de sus servicios de inteligencia y de grupos o personas, que estén dirigidas a la obtención ilegal de información.

- Protección ante emergencias y catástrofes: establecer un sistema nacional de protección de los ciudadanos que garantice una respuesta adecuada ante los distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana, sea esta accidental o intencionada.

- Seguridad marítima: impulsar una política de seguridad en el espacio marítimo con la finalidad de mantener la libertad de navegación y proteger el tráfico marítimo y las infraestructuras marítimas críticas; proteger la vida humana en el mar; prevenir y actuar ante actividades criminales y actos terroristas que se desarrollen en este medio; proteger y conservar el litoral, los recursos del medio marino, el medio ambiente marino y el patrimonio arqueológico sumergido; y prevenir y responder en casos de catástrofes o accidentes en el medio marino.

- Protección de infraestructuras críticas: robustecer las infraestructuras que proporcionan los servicios esenciales para la sociedad.

4.2. Guías prácticas de ciberseguridad en entornos industriales

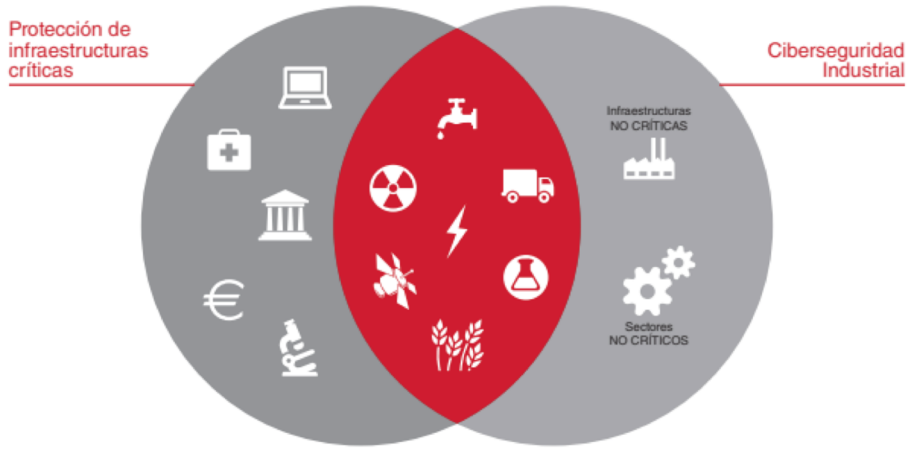
No debemos confundir la protección de las infraestructuras críticas con la ciberseguridad industrial, que podríamos definir (149) como el conjunto de prácticas, procesos y tecnologías diseñadas para gestionar el riesgo (ciberriesgo) derivado del uso, tratamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías. Para tener una visión global y completa, deberemos complementar los aspectos de ciberseguridad industrial, que en definitiva aborda la prevención, monitorización y mejora de la resistencia de los sistemas industriales y su recuperación ante acciones hostiles o inesperadas que puedan afectar al correcto funcionamiento de los procesos e instalaciones industriales, con sus versiones equivalentes en otras dimensiones de la seguridad, como la seguridad medioambiental, la seguridad física y

la seguridad de las personas y sus equipamientos, sin descuidar el patrimonio tecnológico de las industrias, que son el conjunto de activos (tangibles o no) que se pueden derivar del trabajo intelectual (en forma de idea, invención, secreto industrial, proceso, programa, dato, fórmula, patente, *copyright* o marca o aplicación, derecho o registro.

La catalogación final como una infraestructura crítica dependerá, de entrada, del sector en el que la actividad industrial se enmarque, pero siempre será este el principal activo a proteger en el marco de nuestro programa de ciberseguridad industrial (por lo que seguir las recomendaciones en el marco del Programa de Protección de Infraestructuras Críticas siempre es interesante).

En la figura 43 podemos ver, de forma clara, la interrelación entre la protección de infraestructuras críticas y la ciberseguridad industrial.

Figura 43. Ciberseguridad industrial y protección de infraestructuras críticas (150)



Aunque el ámbito de aplicación de las iniciativas de protección de infraestructuras críticas (PIC) (activos fundamentales para la sociedad) es mucho menos extenso, en cuanto al número de infraestructuras afectadas, que el de la ciberseguridad industrial (CI), las iniciativas PIC han alcanzado mucha más relevancia que las iniciativas de CI. Desde el punto de vista de la aproximación a la protección de las organizaciones, PIC tiene un alcance mayor que CI, ya que esta solo se dedica a los procesos industriales (y los sistemas que los soportan), mientras que PIC, además de abarcar sectores que no tienen relación con la industria, incluye aspectos como la seguridad física, ambiental y de las personas, y, en algunos países, el cumplimiento legal. Es precisamente el aspecto legal, y evidentemente la repercusión que tendría sobre la sociedad la alteración o destrucción de las infraestructuras afectadas, lo que ha causado que PIC adquiera mucha más relevancia que la ciberseguridad industrial. Sin embargo, el ámbito de aplicación de la CI es más amplio que el de PIC en los sectores industriales, ya que la gran mayoría de las infraestructuras industriales existentes en el mundo no estarán afectadas por ninguna ley PIC.

Uno de los papeles más importantes desempeñado por PIC ha sido su utilización como un dinamizador de la ciberseguridad industrial debido al cada vez más elevado grado de dependencia de dichas infraestructuras de las tecnologías telemáticas orientadas a la operación y supervisión de sistemas de control y automatización, y su creciente interconexión y dependencia con los sistemas de información y comunicaciones de las organizaciones, así como de internet. De manera similar a como, en España, la Ley orgánica de protección de datos (LOPD) aceleró la implantación de medidas de seguridad de la información en las organizaciones, derivando en muchas ocasiones en la implantación de sistemas de gestión de la seguridad de la información, las leyes relacionadas con la protección de infraestructuras críticas están provocando que, entre las labores requeridas para alcanzar el cumplimiento, se incluyan aspectos relacionados con la ciberseguridad industrial, que de otra manera las organizaciones no hubiesen implantado o lo hubiesen hecho mucho más tarde.

Ambos entornos coinciden en una serie de componentes comunes:

1) La gestión de la ciberseguridad de los componentes tecnológicos, de las infraestructuras (equipos, redes y sistemas en los que se aloja la información). Deben identificarse y valorarse los activos de una organización, identificar las amenazas y vulnerabilidades, estimar la frecuencia de ocurrencia e impactos, y estimar el cálculo de riesgos que pueden sufrir estos dispositivos de control y automatización industrial. Es clave garantizar la integridad de los sistemas de control y automatización industrial y, con ello (si el diseño, implantación y mantenimiento son los adecuados), garantizar su disponibilidad y la gestión que hacen de la información (y toma de decisiones) que sobre la base de ella van a tomar.

2) La gestión de incidentes, que en el caso de las infraestructuras críticas suelen tener un impacto mucho mayor, pero en cualquier caso esta gestión estará condicionada por la naturaleza de la infraestructura, su tamaño y complejidad.

3) El intercambio de conocimiento, que tal y como recomiendan todas las guías de buenas prácticas y planes estratégicos, son un elemento clave para acelerar los avances hacia la protección de las infraestructuras o instalaciones y sistemas industriales. En el caso de la ciberseguridad industrial, al no ser un sector de interés público, el aspecto de la compartición de información y conocimiento no siempre se implementa de forma correcta (151).

4) La evaluación de riesgos, con el fin de determinar sobre qué componentes actuar y qué medidas deben ser adoptadas para disminuir el riesgo afrontado.

5) La gestión de la cadena de suministro, dado que las infraestructuras industriales cada vez están menos aisladas, tanto en el aspecto de sus sistemas y redes como en el aspecto de los procesos con los proveedores, subcontratistas, intermediarios o, incluso, clientes finales. Existe un complejo entramado de interconexiones con otras infraestructuras y agentes, de manera que la inte-

rrupción del suministro de un servicio puede repercutir en los servicios ofrecidos por otras instalaciones, lo que conlleva un control exhaustivo de todas las partes implicadas en la infraestructura. Este control debe afectar a toda la cadena de suministro (extremo a extremo), y no debe descuidar ningún aspecto, pues su repercusión podría ser transmitida a otras cadenas de suministro en un efecto cascada de consecuencias de gran alcance.

6) La gestión de la continuidad de las operaciones, para poder garantizar (por estas interdependencias que indicábamos) la prestación del servicio (en el caso de infraestructuras críticas) o la continuidad del negocio y la propia supervivencia de la organización en el caso de los sistemas industriales. Para ello (como ya hemos visto), deberán implantarse las medidas de seguridad y los procedimientos que mejoren la recuperación frente a interrupciones que, como vimos, se estructura en tres fases:

- Fase 1, de análisis del impacto y de los riesgos, para poder identificar claramente los procesos críticos del negocio.

- Fase 2, de diseño de una estrategia de recuperación, con objetivos de tiempo de recuperación, procedimientos alternativos para cada proceso de negocio, centro de respaldo –propio o subcontratado– y establecimiento de planes de contingencia probados y procedimentados que incluyan tanto la operación a seguir como los recursos técnicos y humanos a utilizar.

- Fase 3, de instalación de recursos en centro de respaldo, formación de los equipos de emergencia y documentación de los procedimientos técnicos de recuperación.

Como caso particular de trabajo en la definición de guías de soporte a la gestión de la ciberseguridad industrial, en el marco del Centro Nacional de Protección de Infraestructuras Críticas, se han hecho de forma extensa guías para la gestión de los sistemas de control industrial que puedan presentar ciertas peculiaridades con respecto a otros sistemas tecnológicos, debido a la importancia que para ellos tiene la operación en tiempo real, y el importante impacto que podría tener cualquier incidente de seguridad sobre ellos. Como podemos ver a continuación, estas guías tienen actualización (no demasiado recientes[153]) (152):

[153]Aunque el tema sigue siendo de interés y actualidad y se sigue trabajando al respecto (230).

- Guía 480 SCADA - Seguridad en sistemas SCADA (153), para presentar la problemática planteada por los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad de controlar su seguridad.

- Guía 480A SCADA - Guía de buenas prácticas (154) para obtener una profunda comprensión de los riesgos a los que se enfrenta el negocio de las amenazas de los sistemas de control de procesos, con el fin de identificar-

los y conducirlos al nivel adecuado de protección de seguridad que se requiere.

- Guía 480B SCADA - Comprender el riesgo de negocio (155) para proporcionar orientación para estudiar el riesgo del negocio y el estudio continuo de este riesgo a partir de las definiciones de la Guía 480A.

- Guía 480C SCADA - Implementar una arquitectura segura (156) para proporcionar orientación para decidir una arquitectura de seguridad adecuada para los sistemas de control de procesos a partir de la Guía 480A.

- Guía 480D SCADA - Establecer capacidades de respuesta (157) para proporcionar orientación a la hora de establecer las capacidades de respuesta relacionadas con las amenazas a la seguridad digital del control de procesos y los sistemas SCADA de acuerdo a las definiciones de la Guía 480A.

- Guía 480E SCADA - Mejorar la concienciación y las habilidades (158) para desarrollar, examinando en detalle cada una de las áreas clave de la Guía 480A, una orientación general sobre la mejora de las habilidades de seguridad en el control de procesos dentro de las organizaciones.

- Guía 480F SCADA - Gestionar el riesgo de terceros (159) para, a partir de la Guía 480A, proporcionar orientación sobre las buenas prácticas de gestión de riesgos de terceros para la seguridad de los sistemas de control de procesos.

- Guía 480G SCADA - Afrontar proyectos (160) para, a partir de la guía 480A, proporcionar orientación de buenas prácticas sobre cómo incluir consideraciones de seguridad en los proyectos de seguridad en control de procesos.

- Guía 480H SCADA - Establecer una dirección permanente (161) para, a partir de la Guía 480A, proporcionar orientación a la hora de definir e implementar los marcos de gobierno adecuados para la seguridad en los sistemas de control de procesos.

5. Legislación y regulación. Infraestructuras críticas

5.1. Infraestructuras críticas (*critical information infrastructure*, CII)

La gestión de la ciberseguridad es de por sí una actividad compleja, pero cuando afecta a infraestructuras críticas, se vuelve crucial. Algunos incidentes más o menos recientes, como el caso del ataque a los sistemas de refrigeración de centrales nucleares para poder impactar en el programa nuclear de Irán, conocido como el caso Stuxnet (162), muestran la criticidad de la gestión de la ciberseguridad en estos entornos, pues una mínima brecha puede tener un impacto casi irreversible de grandes dimensiones.

La gran diferencia entre la ciberseguridad industrial y la protección de infraestructuras críticas radica en el punto de que la segunda afecta a la seguridad nacional, con lo que la mayoría de los procedimientos y métodos de implantación están basados en la obligatoriedad del cumplimiento legislativo.

Actualmente, en el caso de la ciberseguridad industrial, se tiene siempre en consideración la mejora de la eficiencia de las operaciones; en el caso de la protección de las infraestructuras críticas, muchas veces se acaba con la protección de la infraestructura sin entrar en aspectos de eficiencia. Con todo, dada la consciencia de un mundo sostenible, cada vez se irán introduciendo también estos conceptos en la protección de infraestructuras críticas.

La sociedad en la que estamos comporta una completa interdependencia entre muchos de los sistemas que prestan los servicios fundamentales de nuestra actividad diaria, como pueden ser todos los aspectos relacionados con los suministros y las comunicaciones (en sentido amplio, de transporte, de información, de telecomunicación…). Algunas de las infraestructuras que dan soporte a estos servicios son de gestión pública, otras de gestión privada, y también las tenemos de gestión mixta. Por otro lado, evidentemente, los modelos de gestión en cada estado pueden ser diferentes, pero al final el propio proceso de suministro del servicio se vuelve global, conllevando una clara interrelación entre los sectores público y privado para la provisión de forma segura del servicio.

Podríamos definir (147) las infraestructuras críticas como las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información cuyo funcionamiento es indispensable y no permite soluciones alternativas. La perturbación o destrucción de cualquiera de estos activos puede tener un impacto directo sobre la seguridad nacional y afectar, por ejemplo, a la estabilidad financiera, a la salud pública o a una combinación de estas dimensiones de la

seguridad. La fuerte interrelación y complejidad de dichos sistemas que dan soporte a los servicios públicos conlleva que la caída de una (sola) infraestructura crítica pueda originar una cascada de efectos negativos, al arrastrar en cadena a otros sistemas o instalaciones con consecuencias lesivas sobre servicios básicos para la población o/y el funcionamiento del Estado (del bienestar).

Estas infraestructuras que proveen estos servicios básicos se consideran críticas en el sentido de que la interrupción o disfunción de su funcionamiento derivaría en importantes efectos sobre el desarrollo esperado de las actividades de la vida diaria de la sociedad, y tendrían un impacto mayúsculo.

En el marco de la legislación española, se define como ámbitos de especial interés de la seguridad nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley (163) serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

Claro es, pues, que este es un aspecto de la ciberseguridad que solo puede articularse si se define una estrategia que se sustente sobre un marco de referencia global y que contemple todos los aspectos posibles en materia de seguridad. Tal y como se indica en la Estrategia de Seguridad Nacional 2013 (164), deben tenerse en consideración todas las singularidades de los riesgos y amenazas a los que se enfrenta la sociedad, para poder dar respuesta de forma flexible y eficaz, pero con la limitación propia de recursos. Debe enfocarse la acción hacia las actuaciones de prevención, de protección y de respuesta en un entorno altamente complejo.

En el contexto de la ciberseguridad, el problema si cabe se vuelve aún más global e interconectado, en tanto nos movemos en un terreno que se está regulando de forma continuada y acelerada, donde el control es muy difícil, por lo que en todos los estados se están definiendo estrategias referentes a la ciberseguridad y la gestión de las infraestructuras críticas.

5.2. Legislación

5.2.1. Ley PIC (España)

La definición de una Ley para la protección de las infraestructuras críticas se fundamenta en la Ley 8/2011, de 28 de abril (165), si bien podríamos indicar la puesta en marcha del Centro Criptológico Nacional (166) (CCN) en 2004 (167), adscrito al Centro Nacional de Inteligencia.

Las infraestructuras críticas existentes en un estado se agrupan dentro de sectores estratégicos: aquellos que son esenciales para la seguridad nacional o para el conjunto de la economía de un país (defensa, energía, aeroespacial, nuclear, administrativo, financiero, etc.). La protección de las infraestructuras críticas surge como respuesta de los gobiernos a la necesidad de proteger el complejo sistema de infraestructuras que dan soporte y posibilitan el normal funcionamiento de los sectores productivos, de gestión y de la vida ciudadana en general. Para ello, los distintos países han abordado dicha problemática bajo distintas perspectivas, que se pueden resumir en:

1) Establecimiento de un marco normativo estricto;

2) Fomento de las relaciones público-privadas;

3) Establecimiento de un marco normativo básico acompañado de una serie de medidas para fomentar las relaciones público-privadas.

En cualquier caso, el objetivo fundamental de la protección de las infraestructuras críticas es el desarrollo, implantación o mejora de las medidas de seguridad oportunas, tanto en su vertiente física como lógica/cibernética, que deben acometer los operadores propietarios o responsables de su gestión, de cara a garantizar un nivel de protección adecuado.

La política de seguridad nacional, en el marco del Estado español, queda claramente expuesta, (163) en tres ejes:

1) La política de seguridad nacional es una política pública, bajo la dirección del presidente del Gobierno, bajo la responsabilidad del Gobierno de España, en la que participan todas las administraciones públicas.

2) Los principios básicos que van a orientar la política de seguridad nacional son la unidad de acción, anticipación, prevención, eficiencia y sostenibilidad en el uso de recursos, capacidad de resistencia y recuperación, coordinación y colaboración (como podemos ver en la figura 44).

Figura 44. Definición de seguridad nacional

- **Unidad de acción** (147), que supone la implicación, la coordinación y la armonización de todos los actores y los recursos del Estado bajo la dirección del presidente del Gobierno, así como la colaboración público-privada y la implicación de la sociedad en general. El enfoque integral de la seguridad, comprensivo de todas sus dimensiones, justifica este principio de acción y precisa, a su vez, de una gestión completa a través de un sistema de seguridad nacional impulsado y liderado por el presidente del Gobierno.

- **Anticipación y prevención**, que han de orientar la acción del Gobierno a la detección y la reconducción de situaciones que pueden representar un potencial riesgo o amenaza para la seguridad nacional.

- **Eficiencia y sostenibilidad en el uso de los recursos**, un principio que, si bien debe presidir en todo momento la actuación administrativa, cobra especial significación en un contexto como el presente. Se sustenta en la priorización de los recursos y la optimización de su empleo, precisa el control y la evaluación de los resultados y orienta la organización administrativa.

- **Resiliencia o capacidad de resistencia y recuperación**, principio relativo a la aptitud de los recursos humanos y materiales para afrontar con flexi-

bilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus consecuencias negativas.

3) La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la política de seguridad nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas[154] que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley. Los cuatro principios rectores de la Estrategia son la unidad de acción, la anticipación, la eficiencia y la resiliencia, como vemos en la figura 45.

[154]Definidos en el capítulo 3 de la Estrategia de Seguridad Nacional.

Figura 45: Principios rectores de la Estrategia de Seguridad Nacional 2017

En una clara visión de colaboración con el sector privado, y muy especialmente en el ámbito de las infraestructuras críticas, se concibe la colaboración con las entidades privadas en materia de seguridad nacional siempre que las circunstancias así lo aconsejen, y siempre que sean operadoras de servicios esenciales y de infraestructuras críticas que puedan, por lo tanto, afectar seriamente a la seguridad nacional. Las formas y los mecanismos de la colaboración entre el sector privado y el sector público se definirán de forma reglamentaria por el Gobierno de España.

En materia de seguridad nacional, los órganos competentes son:

- Las Cortes Generales.
- El Gobierno.

- El presidente del Gobierno.
- Los ministros.
- El Consejo de Seguridad Nacional.
- Los delegados del Gobierno en las comunidades autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla.

El Sistema de Seguridad Nacional (163) es el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de seguridad nacional ejercer sus funciones. En el Sistema de Seguridad Nacional se integran los componentes fundamentales siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada.

Las funciones reguladas del Sistema de Seguridad Nacional son:

- Evaluar los factores y situaciones que puedan afectar a la seguridad nacional.
- Recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley.
- Detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las administraciones públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema.

La Estrategia de Seguridad Nacional se va revisando de forma periódica para garantizar que siempre se tienen en consideración las evoluciones en materia de ciberseguridad (tanto desde la perspectiva de la defensa y la prevención como de la perspectiva de las vulnerabilidades y amenazas y técnicas, digamos, de ataque). En este sentido, es bueno tener la referencia de los últimos documentos de la política estratégica nacional en materia de ciberseguridad:

- Estrategia de Seguridad Nacional 2011 (168).
- Estrategia de Seguridad Nacional 2013.
- Estrategia de Seguridad Nacional 2017 (169).

Uno de los ámbitos de actuación de máxima prioridad de la Estrategia de Seguridad Nacional son las infraestructuras críticas, que se desglosan en siete líneas de actuación estratégica:

1) Responsabilidad compartida y cooperación público-privada (170). Es imprescindible que tanto las administraciones públicas como los operadores privados asuman la responsabilidad correspondiente y trabajen, de forma coordinada, en la protección de las infraestructuras críticas en todo momento. El Gobierno promoverá la creación de un sistema que comprenda a todos los agentes responsables y facilitará los canales y procedimientos de comunicación seguros que hagan posible la cooperación mutua y el intercambio de información de interés para todas las partes.

2) Planificación escalonada. Se impulsará un sistema de planificación escalonada que permita identificar, evaluar, prevenir y mitigar los riesgos a los que nos enfrentamos, desde la perspectiva más global y estratégica, hasta aquellos activos que se encuentren bajo la responsabilidad de un operador u organización. Este sistema se abordará a partir de un enfoque integral multirriesgo y homogeneizador.

3) Equilibrio y eficiencia. El Gobierno aplicará una metodología homogénea que permitirá concentrar los esfuerzos sobre las áreas más vitales: catalogará las infraestructuras de manera priorizada y permitirá una racionalización en la asignación de recursos.

4) Resiliencia. Más allá de las medidas que doten a los activos críticos de una mayor seguridad, las políticas en materia de protección de infraestructuras críticas deberán promover las acciones necesarias con el fin de lograr un incremento de la capacidad de los sistemas que les permita seguir operando, pese a estar sometidos a un ataque o incidente, aun cuando sea en un estado degradado o debilitado. En este sentido, se debe contemplar la existencia de sistemas redundantes o aislados y la adecuada dotación de elementos de reposición.

5) Coordinación. La gestión de crisis, en el ámbito gubernamental, organizará todas las tareas, responsabilidades y recursos existentes teniendo en cuenta las infraestructuras críticas como parte integrante en las fases de preparación, respuesta y recuperación. Resulta esencial la existencia de una adecuada coordinación operativa entre las organizaciones responsables de la gestión de riesgos y la gestión de crisis.

6) Cooperación internacional. Se impulsará el cumplimiento del Programa Europeo de Protección de Infraestructuras Críticas (EPCIP) (171) y de la Directiva Europea 2008/114/CE (172) del Consejo, sobre la identificación y designación de infraestructuras críticas europeas y evaluación de la necesidad de mejorar su protección. Ambos instrumentos se entienden como los mejores medios para lograr la consecución de la cooperación de los países europeos y la pro-

tección de nuestros intereses nacionales. De la misma manera, se favorecerá la existencia de canales internacionales de información, alerta temprana y respuesta, así como la participación activa en foros internacionales.

7) Garantía en la seguridad de las infraestructuras críticas conforme a lo expuesto en el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC). Se dotará a estas instalaciones de sistemas redundantes e independientes de otras tecnologías y operadores, dado que sobre ellas descansa el funcionamiento de los servicios esenciales.

Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)

No es hasta 2007 cuando se puede concretar la política de seguridad nacional del Gobierno de España con la creación del Centro Nacional de Protección de Infraestructuras Críticas (173) como órgano responsable (174) del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior, en dependencia de la Secretaría de Estado de Seguridad, que es el máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

Una de sus funciones es la información del nivel de riesgo nacional[155] en el que nos encontramos en cada momento, como podemos ver en la figura 46 (para octubre de 2018).

[155] Son los conocidos como niveles de alerta en infraestructuras críticas (NAIC).

[156] Formalmente es un CERT-SI que actúa como CERT para el ámbito de la seguridad e industria, y por lo tanto vinculado a la ciberseguridad industrial y la protección de las infraestructuras críticas nacionales.

Figura 46. Niveles de riesgo definidos por el Centro Nacional de Protección de Infraestructuras Críticas

La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo en el que, entre otros aspectos, se sientan las bases para la colaboración del CNPIC (175) y el Instituto Nacional de Ciberseguridad (176) (INCIBE) en materia de respuesta a incidentes para las tecnologías de la información de las infraestructuras críticas ubicadas en España. De esta forma, el INCIBE se convierte en una herramienta de apoyo al CNPIC en la gestión de incidentes de ciberseguridad, actuando como CERT Gubernamental[156].

Ambas entidades han puesto en marcha un Equipo de Respuesta a Incidentes de Seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica. De este modo, este Equipo de Respuesta se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a escala nacional.

En caso de que una infraestructura crítica sufra un problema de seguridad cibernético, el operador responsable de la misma podrá beneficiarse de los servicios del Equipo de Respuesta, informando de la incidencia a través del punto de contacto único habilitado para esta finalidad.

En este sentido, se entiende por problema de seguridad cibernético cualquier incidente que, empleando o estando dirigido a elementos tecnológicos, afecte al correcto funcionamiento de la infraestructura afectada, como por ejemplo ataques para la parada o inutilización de servicios tecnológicos, acceso a información privilegiada, alteración de información para manipular de forma fraudulenta los sistemas tecnológicos y la información que manejan, etc.

5.2.2. Directivas europeas

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA, European Network and Information Security Agency (177)) tiene, como objetivo, mejorar las redes y la seguridad de la información en la Unión Europea, así como desarrollar una cultura de la ciberseguridad que beneficie a los ciudadanos, a las empresas y al sector público de la Unión Europea. Para ello, ENISA ayuda y aconseja de forma profesional, a través de estudios e investigación, tanto a la Comisión Europea como a los estados miembros. ENISA fue creada en 2004 con el objetivo de mejorar las redes y la seguridad de la información de los distintos estados que forman la Unión Europea. Ese mismo año contempló la aparición de la primera iniciativa europea relacionada con la protección de infraestructuras críticas, mediante la comunicación de la Comisión al Consejo y el Parlamento Europeo (COM(2004) 702) (178), titulada «Protección de Infraestructuras Críticas en la lucha contra el terrorismo». El efecto de esta comunicación fue la creación, a finales de 2004, de EPCIP (European Programme for Critical Infrastructure Protection (179)) para la coordinación de esfuerzos público-privados entre naciones en la protección de infraestructuras críticas, de CIWIN (Critical Infrastructure Warning Information Network (180)) para el intercambio de conocimiento relacionado con la protección de infraestruc-

turas críticas y la edición de la directiva EU COM(2006) 768 (181), que obliga a todos los estados miembros a transponer los componentes de EPCIP dentro de sus estatutos nacionales. En noviembre de 2005, la Comisión presentó en un comunicado (COM(2005) 576) el Libro Verde (182) «Sobre un programa europeo para la protección de infraestructuras críticas», en el que se recababan puntos de vista en torno a las posibles opciones para el EPCIP.

Los objetivos del conjunto de directivas en este ámbito, por parte del Consejo de la Unión Europea, son:

- La identificación de infraestructuras críticas europeas (ICE). Cada estado debe identificar las infraestructuras críticas existentes en su territorio.

- La designación de las ICE. Los estados deben informar al resto de estados afectados por la designación de una ICE, así como a la Comisión y al propietario u operador anualmente.

- La definición y concreción en planes de seguridad del operador. Cada estado debe asegurarse de que las ICE disponen de un plan de seguridad del operador, garantizando su aplicación en el plazo de un año tras la designación de ICE.

- La identificación de un responsable de enlace. Cada estado debe asegurarse de que las ICE disponen de un responsable de enlace para la seguridad, así como de que existen los mecanismos de comunicación adecuados.

- La generación y gestión de informes. Cada estado ha de realizar una evaluación de amenazas sobre los subsectores de las ICE y presentar a la Comisión, cada dos años, los resultados sobre los riesgos en cada sector.

5.2.3. Ejemplos de otros países

Estados Unidos

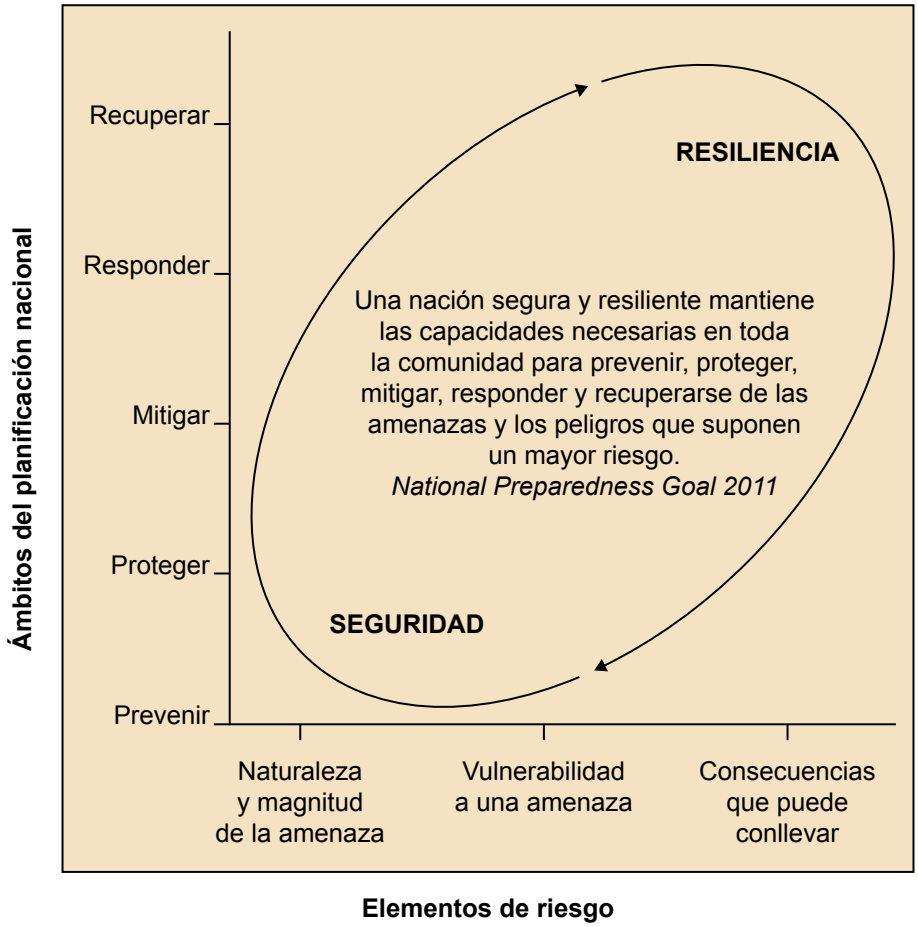
No hay duda del papel referente de Estados Unidos respecto a la sensibilización de la protección de las infraestructuras críticas. Ya en 1995 (183) se declaraba la necesidad de crear un comité para revisar las vulnerabilidades de las infraestructuras críticas de la nación ante posibles ataques terroristas que, por ejemplo, derivó en la Directiva 63 (184) para garantizar que se estará preparado para defender de forma adecuada las infraestructuras críticas de la nación.

Se definen las infraestructuras críticas como aquellos sistemas físicos y basados en el ciberespacio que son esenciales para las operaciones de mínimos de la economía y del gobierno (americanos). Se incluyen, sin limitarse, las teleco-

municaciones, la energía, los bancos y las finanzas, el transporte, los sistemas de suministro de agua y los servicios de emergencia (tanto gubernamentales como privados).

Se define el rol del National Infrastructure Protection Center (185) (NIPC) como estructura para gestionar en un procedimiento cíclico y de continuada revisión (como vemos en la figura 47):

Figura 47. Gestión cíclica de los mecanismos de protección definidos en el Plan Nacional de Protección de Infraestructuras de 2013



- Los procedimientos de análisis de vulnerabilidades, para todos aquellos sectores de la economía o del gobierno que puedan ser objeto de un ataque a sus infraestructuras.

- Los planes de contingencia que puedan identificar los tempos de las respuestas a incidentes de seguridad, las responsabilidades en cada elemento de la cadena de protección de los activos, y la generación (obtención y gestión) de los fondos para su financiación.

- La puesta en marcha de un centro (nacional) de alertas de seguridad que se dedique de forma específica a las infraestructuras críticas, donde se va a potenciar de forma importante la participación del sector privado.

- La puesta en marcha de un mecanismo de respuesta ante cualquier posible incidente a una infraestructura crítica, con el objeto de aislar y minimizar el incidente, y su impacto.

- La definición de un proceso de reconstrucción de la infraestructura atacada para su pronta operación bajo mínimos en caso de un ataque exitoso.

- La definición de un programa de sensibilización y de formación en los aspectos (frágiles) de la gestión de la ciberseguridad que tenga especial relación con los errores y descuidos humanos.

- La puesta en marcha de un programa de investigación y desarrollo en el ámbito de la protección de las infraestructuras críticas, con una importante dotación económica, que pueda garantizar los mecanismos de protección en tiempo y forma adecuada, con una vital participación del sector privado.

- La concreción de un proyecto de gestión de la inteligencia para su aplicación en la recolección de información y su posterior análisis en aspectos de amenazas externas (e internas) a las infraestructuras críticas del país.

- El despliegue de los programas de cooperación internacional para aprovechar el marco global y la interrelación entre diferentes administraciones e instituciones gubernamentales en todos los procesos de gestión de la ciberseguridad (en el ámbito de la protección de las infraestructuras críticas).

- La definición y despliegue continuado de los requerimientos normativos y legislativos adecuados para una mejor gestión de las situaciones de riesgo en el ámbito de las infraestructuras críticas.

La concreción de las acciones de este centro se lleva a cabo a través del Plan Nacional de Protección de Infraestructuras (NIPP) (186), que se va revisando de forma continuada con tres objetivos claros (187):

- Identificar, impedir, detectar e interrumpir las amenazas y peligros contra las infraestructuras críticas del país.

- Reducir las vulnerabilidades asociadas a los activos, sistemas y redes implicadas con dichas infraestructuras.

- Mitigar las potenciales consecuencias de incidentes a dichas infraestructuras críticas.

Para lograr estos objetivos, el Plan:

- Identifica de forma clara las prioridades nacionales.

- Trabaja con objetivos claramente definidos.
- Se enfoca a mitigar los riesgos.
- Contempla métricas continuas para poder evaluar la evolución de las contramedidas diseñadas e implementadas.

Figura 48. Evolución de las principales amenazas de las infraestructuras críticas en el marco del Plan Nacional de Protección de Infraestructuras

Como vemos en la figura 48, las principales fuentes de amenazas de infraestructuras críticas identificadas en el NIPP 2013 son:

- Situaciones pandémicas.
- Temporales (situaciones extremas de catástrofes naturales).
- Incidentes, accidentes y fallos tecnológicos.
- Ciberamenazas.
- Actos de terrorismo.

Desde el punto de vista operativo, el Plan Nacional se descompone en una serie de acciones para poder concretar sus objetivos, que son:

1) Acciones orientadas a potenciar la colaboración entre agentes

- Acción 1: Despliegue de prioridades definidas de forma conjunta para identificar y atacar los proyectos de interés nacional.

- Acción 2: Determinar acciones colectivas en las que focalizar los esfuerzos de todos los agentes implicados.

- Acción 3: Potenciar la participación de los agentes locales y regionales para la resolución de proyectos colaborativos de ámbito nacional.

- Acción 4: Definir mecanismos incentivos para mejorar las soluciones de seguridad y resiliencia de las infraestructuras críticas.

2) Acciones orientadas a la innovación en las soluciones y procesos de gestión del riesgo

- Acción 5: Habilitar mecanismos de toma de decisiones sobre la base de los riesgos trabajando en soluciones de mejora de la concienciación global.

- Acción 6: Analizar las dependencias, interdependencias y efectos cascada entre infraestructuras críticas en caso de incidentes de seguridad.

- Acción 7: Identificar, evaluar y dar respuesta de forma anticipada a los efectos cascada que se puedan producir ante situaciones de ataque a una infraestructura crítica (en lo que respecta a acciones con anterioridad al incidente, durante el incidente y *a posteriori*).

- Acción 8: Promover mecanismos para las actuaciones *a posteriori* de un incidente que deben garantizar la provisión del servicio en el punto (local/regional) del incidente.

- Acción 9: Potenciar las acciones de coordinación y asistencia (por ejemplo, tecnológica) o de formación y capacitación (nuevamente, tanto antes como durante o después de un incidente de seguridad).

- Acción 10: Mejorar los mecanismos de seguridad de las infraestructuras críticas y sus mecanismos de resiliencia a partir de proyectos de investigación y desarrollo al respecto (188).

3) Acciones orientadas al análisis de los resultados

- Acción 11: Evaluar la evolución de las contramedidas implantadas sobre la base de una monitorización de los objetivos de cada una de ellas.

- Acción 12: Definir mecanismos para la gestión continuada durante y después de los incidentes, para poder modificar la respuesta definida previa-

mente, para actuar mejor ante el incidente (capacidad de poder modificar el plan original para tener una mejor respuesta).

Bibliografía

1. **Gorelik, Eugene** (2013). «Cloud Computing Models» [tesis en línea]. Working Paper CISL#. MIT. <http://web.mit.edu/smadnick/www/wp/2013-01.pdf>

2. **Abdoulaye, Philippe A.** (2015, 9 de octubre). «How CIOs can reinvent IT with ITaaS» [en línea]. *CIO Magazine*. <https://www.cio.com/article/2986122/cloud-computing/how-cios-can-reinvent-it-with-itaas.html>

3. **Microsoft Azure**. «What is IaaS?» [en línea]. <https://azure.microsoft.com/en-us/overview/what-is-iaas/>

4. **FS-ISAC** (Financial Services Information Sharing and Analysis Center). <https://www.fsisac.com>

5. **NH-ISAC** (National Health Information Sharing and Analysis Center). <https://nhisac.org>

6. **REN-ISAC** (Research and Education Networking Information Sharing and Analysis Center). <http://www.ren-isac.net>

7. **RCISC** (Retail Cyber Intelligence Sharing Center). <https://r-cisc.org>

8. **Freund, Jack; Jones, Jack** (2014). *Measuring and Managing Information Risk: A fair Approach*. Oxford: Butterworth-Heinemann.

9. **Jelen, George** (2001, 13-14 de junio). «SSE-CMM Security Metrics». *NIST and CSSPAB Workshop*. Washington, D.C.

10. **Berinato, Scott** (2005, 1 de julio). «A Few Good Information Security Metrics» [en línea]. *CSO Magazine*. <https://www.csoonline.com/article/2118152/metrics-budgets/a-few-good-information-security-metrics.html>

11. **Miessler, Daniel** (2017, 17 de octubre). «An Information Security Metrics Primer». <https://danielmiessler.com/study/information-security-metrics/>

12. **Shannon, Claude** (1948). «A Mathematical Theory of Communication». *The Bell System Technical Journal* (vol. 27, pág. 379-423, 623-656).

13. **Alien Vault**. <https://www.alienvault.com/>

14. **Marty, Raffael** (2015). *The Security Data Lake*. Sebastopol, CA: O'Reilly Media, Inc.

15. **Cloonan, John** (2017, 11 de abril). «Advanced Malware Detection - Signatures vs. Behavior Analysis» [en línea]. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/opinions/malware-detection-signatures/>

16. **Sweeney, Bill** (2016, 19 de febrero). «Using Predictive Analytics to Identify Cyber Security Risks» [en línea]. *Image and Data Manager*. <https://idm.net.au/article/0010895-using-predictive-analytics-identify-cyber-security-risks>

17. **Ramzan, Zulfikar** (2016, 15-16 de noviembre). «Quick Look: Machine Learning–Cybersecurity Boon or Boondoggle» [en línea]. *RSA Conference. Where the world talks security*. Abu Dhabi. <https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/>

18. **Brownlee, Jason. Machine Learning Mastery**. <https://machinelearningmastery.com/>

19. **Corona, Igino; Biggio, Battista; Maiorca, Davide** (2016, 15 de noviembre). «AdversariaLib: An Open-source Library for the Security Evaluation of Machine Learning Algorithms under Attack» [en línea]. Cornell University. <https://arxiv.org/abs/1611.04786>

20. **Shankar, Ram** (2016, 9 de marzo). «4 trends in security data science» [en línea]. *O'Reilly*. <https://www.oreilly.com/ideas/4-trends-in-security-data-science>

21. **HP Enterprise** (2014). *Internet of Things Research Study* [en línea]. <http://d-russia.ru/wp-content/uploads/2015/10/4AA5-4759ENW.pdf>

22. **Symantec** (2017). *Internet Security Threat Report* [en línea]. <https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf>

23. **OWASP** (2018). *Open Web Application Security Project* [en línea]. <https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project>

24. **OWASP** (2018). *IoT Attack Surface Areas* [en línea]. <https://www.owasp.org/index.php/IoT_Attack_Surface_Areas>

25. **GSMA** (2016). *IoT Security Guidelines. Overwiev Document* [en línea]. GSM Association. <https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf>

26. **Scully, Padraig** (2017, 19 de enero). «Understanding IoT Security – Part 2 of 3: IoT Cyber Security for Cloud and Lifecycle Management» [en línea]. IOT Analytics. <https://iot-analytics.com/understanding-iot-cyber-security-part-2/>

27. **Hayslip, Gary** (2018, 21 de febero). «Building a cybersecurity strategic plan» [en línea]. CSO. <https://www.csoonline.com/article/3257230/data-protection/building-a-cyber-security-strategic-plan.html>

28. **National Security Authority** (2015). *Action Plan for the Implementation of the Cybersecurity Concept of the Slovak Republic for 2015-2020* [en línea]. Bratislava, Eslovaquia. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ActionPlanfortheImplementationoftheCyberSecurityConceptoftheSlovakRepublic-for20152020 _3_.pdf>

29. **Computer Security Resource Center** (2015, 30 de octubre). *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* [en línea]. CSRC, NIST. <https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CSIP>

30. **NIST (National Institute of Standards and Technology)** (2018). *Information and Communications Technology Supply Chain Risk Management (ICT SCRM)* [en línea]. <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf>

31. **Resilinc Corporation**. <https://www.resilinc.com>

32. **Jones, Andy; Ashendene, Debi** (2005). *Risk Management for Computer Security, Protecting your Network and Information Assets*. Oxford: Butterworth-Heinemann.

33. **InfoSec** (2018). *IT Security Standards and Best Practices* [en línea]. <https://www.infosec.gov.hk/english/technical/standards.html>

34. **Ippolito, L. M.; Wallace, D.** (1995). *A Study on Hazard Analysis in High Integrity Software Standards and Guidelines* [en línea]. NIST Interagency/Internal Report (NISTIR) – 5589. <https://www.nist.gov/publications/study-hazard-analysis-high-integrity-software-standards-and-guidelines>

35. **ISO (International Organization for Standardization)** (2018). *Risk Management Guidelines* [en línea]. ISO 31000:2018. <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en>

36. **ISO** (2012). *Societal security – Business continuity management systems – Requirements* [en línea]. ISO 22301:2012. <https://www.iso.org/standard/50038.html>

37. **Sharp, John** (2012). *Moving from BS 25999-2 to ISO 22301. The new international standard for business continuity management systems* [en línea]. Londres: The British Standard Institution (BSI). <https://www.bsigroup.com/Documents/iso-22301/resources/BSI-BS25999-to-ISO22301-Transition-UK-EN.pdf>

38. **ISO** (2012). *Societal security – Business continuity management systems – Guidance* [en línea]. ISO 22313:2012. <https://www.iso.org/standard/50050.html>

39. **Information Systems Audit and Control Association (ISACA)**. <https://www.isaca.org>

40. **ISACA**. Certified Information Systems Auditor (CISA). <http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx>

41. **ISACA**. Certified Information Security Manager (CISM). <http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx>

42. **ISACA**. Certified in Risk and Information Systems Control (CRISC). <http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx>

43. **ISACA**. Certified in the Governance of Enterprise IT (CGEIT). <http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx>

44. **ISACA**. COBIT 4.1: Framework for IT Governance and Control. <https://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>

45. **ISO**. Conjunto de Estándares de la serie 27000 [en línea]. <https://www.iso.org/search.html?q=2700&hPP=10&idx=all_en&p=0&hFR[category][0]=standard >

46. **Risk World**. <http://www.riskworld.com/>

47. **The Security Risk Analysis Directory**. *COBRA ISO17799 Security Consultant* [en línea]. <http://www.security-risk-analysis.com/cobprods.htm>

48. **Risk Watch**. <https://www.riskwatch.com>

49. **CERT Coordination Center**. <http://www.cert.org/ortave.faq.html>

50. **ENISA**. CRAMM (CCTA Risk Analysis and Management Method) [en línea]. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html>

51. **Global Risk**. *Firm Risk* [en línea]. <https://globalrisk.com/products/firm-risk/>

52. **US Department of Commerce**. <https://www.usa.gov/federal-agencies/u-s-department-of-commerce>

53. **NIST** (2011). *Managing Information Security Risk Organization. Mission, and Information System View* [en línea]. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

54. **NIST** (2012). *Guide for Conducting Risk Assessments* [en línea]. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

55. **ISO**. *ISO27000* [en línea]. <http://www.iso27000.es/iso27000.html>

56. **ISO**. <https://www.iso.org/store.html>

57. **IEC (International Electrotechnical Commission)**. <https://webstore.iec.ch>

58. **ISO/IEC (2018).***ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary* (5.ª ed.) [en línea]. <http://www.iso27001security.com/html/27000.html>

59. **ISO/IEC**. *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27001.html>

60. **ISO/IEC**. *ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems* (3.ª ed.) [en línea]. <http://www.iso27001security.com/html/27006.html>

61. **ISO/IEC**. *ISO/IEC27009:2016 – Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements* [en línea]. <http://www.iso27001security.com/html/27009.html>

62. **ISO/IEC**. *ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27002.html>

63. **ISO/IEC**. ISO/IEC 27003:2017 – Information technology – Security techniques – Information security management system – Guidance (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27003.html>

64. **ISO/IEC**. ISO/IEC 27004:2016 – Information technology – Security techniques – Information security management — Monitoring, measurement, analysis and evaluation (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27004.html>

65. **ISO/IEC**. *ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management* (3.ª ed.) [en línea]. <http://www.iso27001security.com/html/27005.html>

66. **ISO/IEC. ISO/IEC 27007:2017 – Information technology – Security techniques – Guidelines for information security management systems auditing** (2.ª ed.). [en línea]. <http://www.iso27001security.com/html/27007.html>

67. **ISO/IEC**. *ISO/IEC TR 27008:2011 – Information technology – Security techniques – Guidelines for auditors on information security controls* [en línea]. <http://www.iso27001security.com/html/27008.html>

68. **ISO/IEC**. *ISO/IEC 27013:2015 – Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27013.html>

69. **ISO/IEC**. *ISO/IEC 27014:2013 – Information technology – Security techniques – Governance of information security* [en línea]. <http://www.iso27001security.com/html/27014.html>

70. **ISO/IEC**. *ISO/IEC TR 27016:2014 – Information technology – Security techniques – Information security management – Organizational economics* [en línea]. <http://www.iso27001security.com/html/27016.html>

71. **ISO/IEC**. *ISO/IEC 27021:2017 – Information technology – Security techniques – Competence requirements for information security management systems professionals* [en línea]. <http://www.iso27001security.com/html/27021.html>

72. **ISO/IEC**. *ISO/IEC 27010:2015 – Information technology – Security techniques – Information security management for inter-sector and inter-organisational communications* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27010.html>

73. **ISO/IEC**. *ISO/IEC 27011:2016 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations* [en línea]. <http://www.iso27001security.com/html/27011.html.>

74. **ISO/IEC**. *ISO/IEC 27017:2015 / ITU-T X.1631 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services* [en línea]. <http://www.iso27001security.com/html/27017.html>

75. **ISO/IEC.** *ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors* [en línea]. <http://www.iso27001security.com/html/27018.html>

76. **ISO/IEC**. *ISO/IEC 27019:2017 – Information technology – Security techniques – Information security controls for the energy utility industry* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27019.html>

77. **ISO/IEC**. *ISO/IEC TR 27015:2012 – Information technology – Security techniques – Information security management guidelines for financial services* [en línea]. <http://www.iso27001security.com/html/27015.html>

78. **ISO/IEC**. *ISO/IEC TR 27023:2015 – Information technology – Security techniques – Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002* [en línea]. <http://www.iso27001security.com/html/27023.html>

79. **ISO/IEC**. *ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity* [en línea]. <http://www.iso27001security.com/html/27031.html>

80. **ISO/IEC**. *ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity* [en línea]. <http://www.iso27001security.com/html/27032.html>

81. **ISO/IEC**. *ISO/IEC 27033:2010+ – Information technology – Security techniques – Network security* (6 partes) [en línea]. <http://www.iso27001security.com/html/27033.html>

82. **ISO/IEC**. *ISO/IEC 27034:2011+ – Information technology – Security techniques – Application security* (todas excepto parte 4 publicada) [en línea]. <http://www.iso27001security.com/html/27034.html>

83. **ISO/IEC**. *ISO/IEC 27035:2016 – Information technology – Security techniques – Information security incident management* (parte 1 y 2 publicadas) [en línea]. <http://www.iso27001security.com/html/27035.html>

84. **ISO/IEC**. *ISO/IEC 27036:2013+ – Information technology – Security techniques – Information security for supplier relationships* (cuatro partes) [en línea]. <http://www.iso27001security.com/html/27036.html>

85. **ISO/IEC**. *ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence* [en línea]. <http://www.iso27001security.com/html/27037.html>

86. **ISO/IEC**. *ISO/IEC 27038:2014 – Information technology – Security techniques – Specification for digital redaction* [en línea]. <http://www.iso27001security.com/html/27038.html>

87. **ISO/IEC**. *ISO/IEC 27039:2015 – Information technology – Security techniques – Selection, deployment and operation of intrusion detection and prevention systems (IDPS)* [en línea]. <http://www.iso27001security.com/html/27039.html>

88. **ISO/IEC**. *ISO/IEC 27040:2015 – Information technology – Security techniques – Storage security* [en línea]. <http://www.iso27001security.com/html/27040.html>

89. **ISO/IEC**. *ISO/IEC 27041:2015 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods* [en línea]. <http://www.iso27001security.com/html/27041.html>

90. **ISO/IEC**. *ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence* [en línea]. <http://www.iso27001security.com/html/27042.html>

91. **ISO/IEC**. *ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes* [en línea]. <http://www.iso27001security.com/html/27043.html>

92. **ISO/IEC**. *ISO/IEC 27050:2016+ – Information technology – Security techniques – Electronic discovery* (parte 1 y 3 publicadas) [en línea]. <http://www.iso27001security.com/html/27050.html>

93. **ISO/IEC**. *ISO/IEC TR 27103:2018 – Information technology – Security techniques – Cybersecurity and ISO and IEC standards* [en línea]. <http://www.iso27001security.com/html/27103.html>

94. **ISO**. *ISO 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002* (2.ª ed.) [en línea]. <http://www.iso27001security.com/html/27799.html>

95. **ISA (International Society of Automation)** . <https://www.isa.org/>

96. **ISA**. *Technical Topics*. <https://www.isa.org/technical-topics/>

97. **ISA**. *ISA95, Enterprise-Control System Integration*. <https://www.isa.org/isa95/>

98. **Williams, Theodore J.** (ed.) (1989). *A Reference Model for Computer Integrating Manufacturing (CIM). A description from the Viewpoint of Industrial Automation* [en línea]. CIM Reference Model Committee. International Purdue Workshop on Industrial Computer Systems. <http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.pdf>

99. **IEEE 802.11**™. IEEE 802.11™ Wireless Local Area Networks. <http://www.ieee802.org/11/>

100. **ISA**. *ISA100, Wireless Systems for Automation*. <https://www.isa.org/isa100/>

101. **Lennvall, Tomas; Svensson, Stefan; Hekland, Fredrik** (2008, 7 de octubre). «A Comparison of WirelessHART and ZigBee for Industrial Applications». *2008 IEEE International Workshop on Factory Communication Systems*. Dresde, Alemania.

102. **ISA**. *ISA50, Signal Compatibility of Electrical Instruments* [en línea]. <https://www.isa.org/isa50/>

103. **B&B Electronics**. *An Introduction to Industrial Ethernet* [en línea]. B&B White Paper núm. BB-WP12b-R1-1112. <http://bb-smartpartners.com/pdf/whitePapers/AnIntroductionToIndustrialEthernet-WP12B-R1_1112.pdf>

104. **Profibus**. <https://www.profibus.com/>

105. **EtherCat**. <https://www.ethercat.org/default.htm>

106. **Anybus**. <https://www.anybus.com/>

107. **Schneider Electric**. «What is Modbus and How does it work?» [en línea]. <https://www.schneider-electric.co.in/en/faqs/FA168406/>

108. **ISA**. *ISA88, Batch Control* [en línea]. <https://www.isa.org/isa88/>

109. **ISA**. *ISA95, Enterprise-Control System Integration* [en línea]. <https://www.isa.org/isa95/>

110. **ISA**. *ISA106, Procedure Automation for Continuous Process Operations* [en línea]. <https://www.isa.org/isa106/>

111. **ISA**. *ISA Security Compliance Institute (ISCI)* [en línea]. <https://www.isa.org/news-and-press-releases/isa-insights/2014/march/isa-security-compliance-institute-isci/>

112. **ISA Secure**. <https://www.isasecure.org>

113. **ISA Power Industry Division**. <https://www.isa.org/division/powid/>

114. **ISA**. *ISA84, Instrumented Systems to Achieve Functional Safety in the Process Industries* [en línea]. <https://www.isa.org/isa84/>

115. **IEC**. *Functional Safety and IEC 61508* [en línea]. <https://www.iec.ch/functionalsafety/>

116. **Yozallinas, John** (2017, 7 de marzo). «CFSE. Functional Safety Standards - IEC 61508 vs. IEC 61511» [en línea]. Exida. <https://www.exida.com/Blog/functional-safety-standards-iec-61508-vs.-iec-61511>

117. **ISA**. *ISA99, Industrial Automation and Control Systems Security* [en línea]. <https://www.isa.org/isa99/>

118. **WIB (The process Automation User' Association)**. <https://www.wib.nl/>

119. **NERC**. *CIP Standards* [en línea]. <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

120. **IEC**. *TC 65 Industrial-process measurement, control and automation* [en línea]. <https://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2612,25>

121. **Incibe** (2015, 25 de mayo). «IEC 62443: Evolución de la ISA 99» [en línea]. Incibe. <https://www.certsi.es/blog/iec62443-evolucion-isa99>

122. **Ristaino, Andre** (2016, mayo-junio). «Industrial automation cybersecurity conformity assessments» [en línea]. *InTech Magazine*. <https://www.isa.org/intech/20160602/>

123. **Ristaino, Andre** (2016). «Industrial automation cybersecurity conformity assessments» [en línea]. ISA Secure. <https://isasecure.org/en-US/Articles/Industrial-automation-cybersecurity-conformity-ass>

124. **ISA**. *ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* [en línea]. <https://www.isa.org/store/ansi/isa-62443-1-1-990101-2007-security-for-industrial-automation-and-control-systems-part-1-1-terminology,-concepts,-and-models/116720>

125. **Phinney, Tom** (s. f.). IEC 62443: *Industrial Network and System Security* [en línea]. <https://www.isa.org/pdfs/autowest/phinneydone>

126. **IEC**. *SC 65E Devices and integration in enterprise systems* [en línea]. <https://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:12444,25>

127. **IEC**. *IEC TR 62443-3-1:2009 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems* [en línea]. <https://webstore.iec.ch/publication/7031>

128. **IEC**. *IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* [en línea]. <https://webstore.iec.ch/publication/7033>

129. **IEC**. *IEC 62443-3-3:2013/COR1:2014 Corrigendum 1 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* [en línea]. <https://webstore.iec.ch/publication/7032.>

130. **Siemens** (2017). *Managing your Risk: How security establishes a suitable environment for safety* [en línea]. <https://www.industry.siemens.com/topics/global/en/safety-integrated/process-safety/Documents/EN-Whitepaper_Managing-Your-Risk.pdf>

131. **Cosman, Eric** (2018, 3 de abril). «New 62443 Standards Define Requirements for Suppliers» [en línea]. ARC Advisory Group. <https://www.arcweb.com/blog/new-62443-standards-define-requirements-suppliers>

132. **IEC**. *IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements* [en línea]. <https://webstore.iec.ch/publication/33615>

133. **Automation** (2018, 25 de septiembre). «ISA announces ISA/IEC 62443-4-2-2018 standard» [en línea]. <https://www.automation.com/automation-news/article/isa-announces-isaiec-62443-4-2-2018-standard>

134. **ISA**. «Conformity Assessment Programs at ISA» [en línea]. <https://www.isa.org/standards-and-publications/isa-standards/conformity-assessment-programs/>

135. **ISA Secure**. IEC 62443 Conformance Certification. <https://isasecure.org/en-US/>

136. **ISA100 Wireless**. <https://isa100wci.org/>

137. **Collins, Jennifer** (2013). «Nessus Product Names Simplified» [en línea]. Tenable. <https://www.tenable.com/blog/nessus-product-names-simplified>

138. **NIST**. National Vulnerability Database – NVD. <https://nvd.nist.gov/>

139. **Flow Control** (2014). «ISA Security Compliance Institute introduces new cybersecurity certification for industrial automation and process control» [en línea]. <https://www.flowcontrolnetwork.com/isa-security-compliance-institute-introduces-new-cybersecurity-certification-for-industrial-automation-and-process-control/>

140. **Software Engineering Institute (SEI)**. «History of innovation at the SEI» [en línea]. <https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei/index.cfm>

141. **CCN-CERT**. Centro Criptológico Nacional. CERT. <https://www.ccn-cert.cni.es/>

142. **CNN-CERT**. Organismo de Certificación del Centro Criptológico Nacional. <https://www.ccn-cert.cni.es/sobre-nosotros/organismo-certificacion-ccn.html>

143. **ESCERT-UPC**. <https://escert.upc.edu/en>

144. Orden Pre/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. *BOE*, 25 de septiembre de 2007. <https://www.ccn.cni.es/images/stories/normas/pdf/pre_2740_2007_reglamento_evaluacion_certificacion.pdf>

145. Real decreto 951/2015, de 23 de octubre, de modificación del 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/diario_boe/txt.php?id=BOE-A-2015-11881>

146. **CNN-CERT**. Esquema Nacional de Seguridad. <https://www.ccn-cert.cni.es/ens.html>

147. **Gobierno de España** (2013). *Estrategia de Seguridad Nacional. Un proyecto Compartido* [en línea]. Presidencia del Gobierno. Departamento de Seguridad Nacional. <http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf>

148. **Agencia EFE** (2018, 4 de octubre). «La UE, la OTAN y EEUU señalan a Rusia por intentar perpetrar ciberataques globales» [en línea]. <https://www.efe.com/efe/espana/mundo/la-ue-otan-y-eeuu-senalan-a-rusia-por-intentar-perpetrar-ciberataques-globales/10001-3770666>

149. **Centro de Ciberseguridad Industrial (CCI)**. <https://www.cci-es.org/>

150. **CCI** (2013). *La protección de infraestructuras críticas y la ciberseguridad industrial* [en línea]. <https://www.cci-es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218800ca138>

151. **ENISA(European Union Agency for Network and Information Security)** (2011). *Protecting Industrial Control Systems Recommendations for Europe and Member States* [en línea]. <https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>

152. **CNPIC**. *Guías SCADA* [en línea]. <http://www.cnpic.es/Ciberseguridad/4_Guias_Scada/index.html>

153. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480). Seguridad en sistemas SCADA* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480-Seguridad_sistemas_SCADA-mar10.pdf>

154. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480A). Seguridad en el control de procesos y SCADA. Guía de buenas prácticas* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480A-SCADA-Guia_de_buenas_practicas-ene10.pdf>

155. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480B). Seguridad en el control de procesos y SCADA. Guía 1. Comprender el riesgo del negocio* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480B-SCADA-Comprender_el_riesgo_del_negocio-ene10.pdf>

156. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480C). Seguridad en el control de procesos y SCADA. Guía 2. Implementar una arquitectura segura* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480C-SCADA-Implementar_una_arquitectura_segura-ene10.pdf>

157. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480D). Seguridad en el control de procesos y SCADA. Guía 3. Establecer capacidades de respuesta* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480D-SCADA-Establecer_capacidades_de_respuesta-ene10.pdf>

158. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480E). Seguridad en el control de procesos y SCADA. Guía 4. Mejorar la concienciación y las habilidades* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480E-SCADA-Mejorar_la_concienciacion_y_las_habilidades-ene10.pdf>

159. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480F). Seguridad en el control de procesos y SCADA. Guía 5. Gestionar el riesgo de terceros* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480F-SCADA-Gestionar_el_riesgo_de_terceros-ene10.pdf>

160. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480G). Seguridad en el control de procesos y SCADA. Guía 6. Afrontar proyectos* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480G-SCADA-Afrontar_proyectos-ene10.pdf>

161. **CNPIC** (2010). *Guía de seguridad de las TIC (CCN-STIC-480H). Seguridad en el control de procesos y SCADA. Guía 7. Establecer una dirección permanente* [en línea]. <http://www.cnpic.es/Biblioteca/GUIAS_CCN/480H-SCADA-Establecer_una_direccion_permanente-ene10.pdf>

162. **Fruhlinger, Josh** (2017, 22 de agosto). «What is Stuxnet, who created it and how does it work?» [en línea]. CSO. <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>

163. Ley 36/2015, de 28 de septiembre, de seguridad nacional. *BOE*, 29 de septiembre de 2015. <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389>

164. **Gobierno de España** (2013). *Estrategia de Seguridad Nacional. Un proyecto Compartido* [en línea]. Presidencia del Gobierno. Departamento de Seguridad Nacional. <http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional>

165. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *BOE*, 29 de abril de 2011. <https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf>

166. **Centro Criptológico Nacional**. <https://www.ccn.cni.es/index.php/en/>

167. Real decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. *BOE*, 19 de marzo de 2004. <https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf>

168. **CIDOB** (2011). *La Estrategia Española de Seguridad (EES). Una responsabilidad de todos* [en línea]. <https://www.cidob.org/es/publicaciones/serie_de_publicacion/monografias/monografias/la_estrategia_espanola_de_seguridad_ees_una_responsabilidad_de_todos>

169. **Gobierno de España** (2017). *Estrategia de Seguridad Nacional 2017* [en línea]. Gabinete de la Presidencia del Gobierno. Departamento de Seguridad Nacional. <http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017>

170. **Valadés, B.; Marchal, D.** (2016, 19 de diciembre). «Colaboración público-privada, esencial para garantizar la protección de las infraestructuras críticas» [en línea]. *Segurtecnia*. <http://www.seguritecnia.es/revistas/seg/437/index.html?#32>

171. **Comisión Europea** (2005, 17 de noviembre). *Libro verde. Sobre un programa europeo para la protección de infraestructuras críticas* [en línea]. COM(2005) 576 final. Bruselas. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005DC0576&from=ES>

172. 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. *Diario Oficial de la Unión Europea*, 23 de diciembre de 2008. <https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf>

173. **Centro Nacional de Protección de Infraestructuras Críticas**. <http://www.cnpic.es/>

174. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *BOE*, 29 de abril de 2011. <https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630>

175. **Sánchez, Fernando** (2018). «Diez años del CNPIC: pasado, presente y retos de futuro» [en línea]. *Seguritecnia* (núm. 447). <http://www.seguritecnia.es/revistas/seg/447/20/#zoom=z>

176. **Instituto Nacional de Ciberseguridad**. <https://www.incibe.es>

177. **European Network and Information Security Agency**. <https://www.enisa.europa.eu/>

178. **Comisión Europea** (2004, 20 de octubre). *Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism* [en línea]. COM(2004)702. <http://ec.europa.eu/transparency/regdoc/rep/1/2004/EN/1-2004-702-EN-F1-1.Pdf>

179. **Comisión Europea** (2006, 12 de diciembre). *Communication from the Commission on a European Programme for Critical Infrastructure Protection* [en línea]. COM(2006) 786 final. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF>

180. **Comisión Europea** (2018). «Critical Infrastructure Warning Information Network (CIWIN)». <https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en>

181. **EASA** (2006). *Commission Regulation (EC) No 768/2006* [en línea]. <https://www.easa.europa.eu/document-library/regulations/commission-regulation-ec-no-7682006>

182. **Comisión Europea** (2005, 17 de noviembre). *Green Paper on a European programme for critical infrastructure protection* [en línea]. COM(2005)576. <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqh3anpoz1>

183. **President of the United States** (1995). *U.S. Policy on Counterterrorism* [en línea]. Presidential Decision Directives (PDD) NSC-39 (21/6/1995). <https://fas.org/irp/offdocs/pdd39.htm>

184. **President of the United States** (1998). *Critical Infrastructure Protection* [en línea]. Presidential Decision Directives (PDD) NSC-63 (22/5/1998). <https://fas.org/irp/offdocs/pdd/pdd-63.pdf>

185. **National Infrastructure Protection Center**. <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>

186. **Department of Homeland Security** (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* [en línea]. <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>

187. **Department of Homeland Security** (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* [en

línea]. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>

188. **Sánchez Gómez-Merelo, Manuel** (2018, 25 de julio). «Seguridad y Resiliencia en las Infraestructuras Críticas» [en línea]. *Belt*. <http://www.belt.es/expertos/HOME2_experto.asp?id=8341>

189. **Schneier, Bruce** (2016). «The Eternal Value of Privacy» [blog]. <https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html>

190. **SNIA**. *SNIA Dictionary* [en línea]. <https://www.snia.org/education/dictionary>

191. **Kissel, Richard L.** (2013). *Glossary of Key Information Security Terms* [en línea]. NIST Interagency/Internal Report (NISTIR) - 7298rev2. NIST, National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.7298r2>

192. **Bay, Morten** (2016). «What is Cybersecurity? In search of an encompassing definition for the post-Snowden era». *French Journal for Media Research* (núm. 6).

193. **Greenwald, Glenn** (2015). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Nueva York: Metropolitan Books.

194. **Ottis, Rain; Lorents, Peeter** (2010). «Cyberspace: Definition and Implications». *International Conference on Information Warfare and Security*. Cooperative Cyber Defense Centre of Excellence. Tallin (Estonia).

195. **Halter, Vanessa** (2016, 7 de marzo). «Privacy as a Strategic Advantage for Healthcare Products & Services» [en línea]. Healthtech Sidney. <http://www.healthtechsydney.com.au/blog/2016/03/07/privacy-as-a-strategic-advantage-for-healthcare-products-services/>

196. **Imperva Incapsula**. *Advanced Persistent Threat (APT)* [en línea]. <https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html>

197. **Symantec** (2017). *Internet Security Threat Report* 2017.

198. **Zetter, Kim** (2017). «What is Ransomware? A Guide to The Global Cyberattack's Scary Method» [en línea]. Wired (14/5/17). <https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>

199. **Cisco Systems** (2027). *Cisco 2017 Annual Cybersecurity Report* [en línea]. <http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017>

200. **Dimension Data** (2016). *Top 5 cybersecurity trends in 2007* [vídeo en YouTube]. <https://www.youtube.com/watch?v=jy6OrbEKTO0>

201. **AST - Agency for State Technology**. <https://www.ast.myflorida.com/cyber-tips>

202. **Yu, Sounil** (2017, 13-17 de febrero). «Solving Cybersecurity in the Next Five Years: Systematizing Progress for the Short Term». *RSA Conference 2017*. San Francisco.

203. **Mell, Peter M.** (2000, 1 de julio). «Identifying Critical Patches with ICAT». NIST. <https://www.nist.gov/publications/identifying-critical-patches-icat>

204. **NIST**. *NVD - National Vulnerability Database*. <https://nvd.nist.gov/>

205. **CVE - Common Vulnerabilities and Exposures**. <http://cve.mitre.org>

206. **Security Focus**. <https://www.securityfocus.com/>

207. **Verizon Enterprise** (2015). *2015 Data Breach Investigations Report* [en línea]. <https://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf>

208. **Wilson, Tim** (2015, 6 de febrero). «Threat Intelligence Platforms: The Next "Must-Have" for Harried Security Operations Teams" [en línea]. Dark Reading. <https://www.darkreading.com/threat-intelligence-platforms-the-next-must-have-for-harried-security-operations-teams/d/d-id/1320671>

209. **Tittel, Ed** (2017). «Comparing the top threat intelligence services» [en línea]. TechTarget – SeachSecurity. <https://searchsecurity.techtarget.com/feature/Comparing-the-top-threat-intelligence-services>

210. **Beyer, Philip** (2012, 30 de julio). *Risk explained in 5 minutes or less*. SlideShare. <https://www.slideshare.net/pjbeyer/risk-explained-in-5-minutes-or-less>

211. **SecurityMetrics**. <http://securitymetrics.org>

212. **John, Geraint** (2014, julio). *Innovative approaches to supply chain risk*. <https://www.kinaxis.com/sites/default/files/2017-12/innovative-approaches-to-supply-chain-risk-research-scm-world.pdf>

213. **CIO**. <http://www.cio.com>

214. **Grandy, Rick; Serene, Gregg** (2011, 12-17 agosto). «A Report from the Field: Implementing Cyber Security Metrics that Work». *NASA IT Summit*. San Francisco. <https://www.nasa.gov/583318main_2011_Present_NASA_IT_Summit_Grandy_Serene_Implementing_Cyber_Security.pptx>

215. **Microfocus. SPI Dynamics**. <https://software.microfocus.com/en-us/products/webinspect-dynamic-analysis-dast/overview>

216. **Vamos, Robert** (2007, 19 de julio). «HP acquires SPI Dynamics». CNET. <https://www.cnet.com/news/hp-acquires-spi-dynamics/>

217. **Trustwave**. «Trustwave Acquires Cenzic to Enhance Cloud-based Security Testing Platform». <https://www.trustwave.com/en-us/company/newsroom/news/trustwave-acquires-cenzic-to-enhance-cloud-based-security-testing-platform/>

218. **Williams, Christopher** (2007, 6 de junio). «IBM lights on Watchfire». The Register. <https://www.theregister.co.uk/2007/06/06/ibm_watchfire/>

219. **California Department of Health Care Services**. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. <https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/default.aspx>

220. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas*, 23 de noviembre de 1995, núm. L 281. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>

221. **ProserveIT** (2017, 15 de junio). «Security Metrics Program – How It Can Help You Get Your Senior Management's Buy-In!». <http://www.proserveit.com/security-metrics-program/>

222. **Ponemon Institute** (2015, febrero). *2015 Global Megatrends in Cybersecurity* [en línea]. <https://www.raytheon.com/sites/default/files/cyber/rtnwcm/groups/cyber/documents/content/2015_global_megatrends_pdf.pdf>

223. **Scully, Padraig** (2016, 29 de noviembre). «Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers». IOT Analytics. <https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/>

224. **CCN-CERT** (2017). «Actualización del informe de Medidas de seguridad contra el Ransomware». Centro Criptográfico Nacional (13/2/17). <https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/4251-actualizacion-del-informe-de-medidas-de-seguridad-contra-el-ransomware.html>

225. **SEI-CMU** (Software Engineering Institute, Carnegie Mellon University). <https://www.sei.cmu.edu/>

226. **ISO**. *Publicly Available Standards*. <https://standards.iso.org/ittf/PubliclyAvailableStandards/>

227. **DIN**. *JTC1/SC27. ISO/IEC JTC 1/SC 27. IT Security Techniques*. <https://www.din.de/en/meta/jtc1sc27>

228. **ISO**. *ISO/IEC JTC 1/SC 27. IT Security techniques*. <https://www.iso.org/committee/45306.html>

229. **ISO**. *ISO/IEC 27002:2005*. <http://www.iso27000.es/download/ControlesISO27002-2005.pdf>

230. **Foro Internacional Anáhuac** (2017, 21 de octubre). «SCADA: prioridad de la ciberseguridad» [en línea]. *Belt*. <http://www.belt.es/articulos/HOME2_articulo.asp?id=13165>

231. **John, Geraint** (2015, octubre). *The changing face of supply chain risk management*. SCM World: Londres. <http://www.scmworld.com/wp-content/uploads/2017/01/The-Changing-Face-of-Supply-Chain-Risk-Management.pdf>

232. **RiskWatch. ComplianceWatch**. <https://www.riskwatch.com/2013/05/04/compliancewatch>