UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA
Ingeniería de Telecomunicación

PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS ANTE CIBERATAQUES

Alberto Menchén Atienza

Junio 2017

PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS ANTE CIBERATAQUES

AUTOR: Alberto Menchén Atienza
TUTOR: Álvaro Ortigosa

Dpto. Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Junio 2017

Agradecimientos

Quiero agradecer a todo el Equipo de la Escuela Politécnica Superior sus esfuerzos para con mi proyecto.

INDICE DE CONTENIDOS

1 Introducción

1.1 Motivación

Desde hace tiempo, la defensa de los Estados modernos ante el ciber-terrorismo y el ciber-crimen, se ha convertido en una de las principales preocupaciones de los gobiernos actuales. Esto es debido al ciber-terrorismo internacional que, desde hace años, invade nuestro día a día con ataques dirigidos sobre entornos tecnológicos, generalmente contra grandes empresas. Como, por ejemplo, ciberataques contra infraestructuras críticas teniendo graves consecuencias, como el llevado a cabo contra el servidor de dominios Dyn en 2016, que dejó sin servicio a redes sociales y, por tanto, a millones de personas, teniendo esto un gran impacto mediático[1]. Este ataque fue posible llevarlo a cabo utilizando algunos de los dispositivos electrónicos que tenemos en casa, que están conectados con Internet.
Esto significa que electrodomésticos como: el televisor, el microondas, el lavavajillas, la calefacción, el aire acondicionado o las cámaras de video-vigilancia, son susceptibles de ser atacados ya que necesitan el acceso a Internet para el envío y recepción de información. Este tipo de tecnología y comunicaciones, se denomina IoT, Internet of Things. Y forma parte de una nueva forma de acceso a Internet. Y dado que, a priori, estos dispositivos no tendrían información crítica, el usuario no le da la importancia que debería y, por tanto, no se asegura de su protección específica con contraseñas o navegación segura. Siendo actualmente dispositivos fácilmente hackeables y re-utilizables para otros fines.

Partiendo de estas premisas, definiremos el concepto básico sobre el que esta guía tratará: las infraestructuras críticas. Según el BOE del 9 de abril de 2011[2], una infraestructura crítica queda definida como una infraestructura estratégica (instalaciones, redes, sistemas y equipos físicos y de tecnología de la información) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
En este sentido, se pueden distinguir principalmente dos tipos de ciber-ataques contra las infraestructuras críticas: aquellos que tienen como consecuencia la paralización de servicios que tendrían efecto sobre la ciudadanía; y aquellos ataques que tendrían como consecuencia la pérdida de vidas humanas.

Cabe destacar que sólo durante 2015, en España, se produjeron 50.000 incidentes de ciberseguridad, de los cuales 134 fueron contra infraestructuras críticas[3]. Estos ciber-incidentes se han multiplicado por 20 en los últimos 4 años (de 17 a 134 ciberataques en el último año 2015). Y la previsión para el año que viene es que la cifra alcance los 300 ciberataques[2].
Principalmente, estos ataques están dirigidos hacia sectores como energía, agua, sistema financiero, alimentación o logístico. Es decir, se trata de sectores que, si fallan, no habría alternativa para ellos. Son servicios esenciales necesarios para la ciudadanía.

[1] Noticia del diario digital El País del 22 de octubre de 2016.

[2] Boletín Oficial del Estado, con fecha 9 de abril de 2011.

[3] Noticia del diario digital RTVE del 27 de febrero de 2016.

Visto desde el mundo hacker o terrorista, supone todo un desafío poder demostrar sus habilidades y también cuán de vulnerables siguen siendo las empresas hoy en día a este tipo de ciberataques. Pudiendo llegar, una única persona, a provocar un caos absoluto en la población mediante la perturbación o paralización de algún tipo de servicio de los sectores comentados anteriormente. Además, existe el agravante de que, a posteriori, en la mayoría de los casos, nunca se llega a descubrir quién está detrás de cada ciber-ataque y mucho menos el motivo por el cual ha sido realizado.

La mayoría de estos ataques se llevan a cabo aprovechando las vulnerabilidades de los sistemas, que, en muchos casos, su seguridad no se encuentra actualizada o su arquitectura de red no se encuentra securizada de forma óptima.
Y es por esto por lo que la seguridad de los sistemas informáticos se ha convertido en un requisito imprescindible para cualquier empresa o Estado. A lo que hay que añadir la dificultad que tiene el mundo de la tecnología y la velocidad a la que evoluciona, produciendo constantemente avances en este ámbito (*avances que en muchos casos significan sistemas anticuados, vulnerabilidades identificadas," puertas traseras", etc.*). Esto supone un verdadero reto para las empresas y los Estados, ya que requiere grandes inversiones de dinero en materia de seguridad tecnológica que a veces no son invertidos (*sobre todo pequeña y mediana empresa*), provocando que aparezcan y sean descubiertas vulnerabilidades en los sistemas. Sistemas tan importantes como servicios privados online muy famosos, servicios públicos, etc.

Para finalizar este apartado, y después del escenario planteado como antesala de la ejecución de este proyecto, surge la necesidad de generar un estándar a nivel nacional como solución al desarrollo de una estructura de ciber-seguridad a nivel nacional capaz de dar respuesta, tanto los Operadores Críticos como la Administración y Organismos Públicos, y a su vez estén coordinados ante la materialización de ciber-ataques y su prevención. El problema de esta estructura es que, para su desarrollo, se han definido a alto nivel una serie de políticas y procedimientos que dan una visión global pero no ayudan a las empresas detallando específicamente qué actuaciones tienen que llevar a cabo en su día a día (*inventario de activos, inventario de riesgos y amenazas para cada uno de estos activos, desarrollo de una metodología de análisis de riesgos, etc.*). Y es en este sentido, el objetivo de este proyecto: dar solución a este problema y poder cumplir con las exigencias definidas por los organismos competentes: Una guía para la protección de las infraestructuras críticas ante ciber-ataques describiendo todas las actividades a llevar a cabo por la empresa con un gran nivel de detalle, ejemplos, metodologías, desde el inicio, la identificación de las infraestructuras críticas, pasando por la implantación de una metodología de análisis de riesgos y su aplicación sobre el mapa de activos.

1.2 Objetivos

Este proyecto pretende servir de guía para cualquier Organización española que disponga ya de una infraestructura, identificada como crítica por el CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas), ya sea operada o gestionada por la Organización, y

poder adecuarse al marco regulatorio español, la Ley PIC (*Ley para la Protección de las Infraestructuras Críticas*)[4].
Para cumplir con estos requerimientos, es necesario seguir una serie de requisitos a nivel procedimental, desde la generación de una política de seguridad hasta el establecimiento de una serie de Planes (Plan de Seguridad del Operador (PSO) y un Plan de Protección Específico (PPE)), que, entre otros aspectos, deberán incluir un análisis de riesgos, estructuras organizativas en materia de seguridad, y una serie de aspectos relativos a la protección de la infraestructura crítica.
Hoy en día, existen multitud de infraestructuras críticas agrupadas en diversos sectores: bancario, transportes, nuclear, etc. Y cada una de ellas, lleva asociados una serie de riesgos específicos que amenazan su operatividad, ya sea mediante su destrucción o perturbación/alteración de su funcionamiento. Y, según la definición de infraestructura crítica, su perturbación o destrucción tiene consecuencias directas sobre la sociedad y los servicios que presta, algunos de ellos pudiendo ser de primera necesidad como la alimentación o los suministros, electricidad, agua, etc. Para mitigar estos riesgos, desde algunos organismos públicos especializados en materia de seguridad, se han impulsado medidas y planes de protección específicos de cara a implantar controles que prevengan y reaccionen ante la materialización de las amenazas aprovechando las vulnerabilidades de las infraestructuras.
En este proyecto, se establecerán una serie de recomendaciones de cara a profundizar sobre los contenidos mínimos que propone la Ley PIC en los PSO y PPE, ya que, como se ha comentado anteriormente, no detallan las actividades específicas que tiene que llevar a cabo cada empresa para la implementación de las medidas de seguridad (*desde la realización del inventario, incluyendo ejemplos, hasta la implantación de una metodología de riesgos, también con ejemplos incluidos*). Tratando de esta manera que cualquier agente propietario u operador de una infraestructura crítica pueda disponer de una guía para asegurar su infraestructura crítica, asegurando el cumplimiento de una serie de requisitos que comentaremos a continuación.

Finalmente, los pilares del proyecto serán los siguientes: definir los requisitos por los cuales se considera a una infraestructura crítica; establecer los requisitos mínimos que cualquier Operador Crítico deberá cumplir para asegurar el funcionamiento de sus infraestructuras críticas; estudiar y definir riesgos para infraestructuras críticas debido a un ciberataque mediante una metodología de análisis de riesgos y la definición de la seguridad lógica que deberá ponerse en marcha y que todo Operador Crítico deberá cumplir para la mitigación de los riesgos ante un ciberataque. Esto se realizará a través de los diferentes planes y buenas prácticas recomendadas desde los diferentes organismos competentes en este ámbito. Entre estos organismos, podemos destacar los siguientes:

- AEI Seguridad (Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información
- INCIBE (Instituto Nacional de Ciberseguridad de España)
- CERT de Seguridad e Industria (Centro de Respuesta a incidentes de ciberseguridad)
- CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas)
- CCN (Centro Criptológico Nacional)

[4] Boletín Oficial de Estado – Se aprueba la Ley PIC (protección de infraestructuras críticas)

1.3 Organización de la memoria

A continuación, este proyecto avanzará presentando algunas infraestructuras críticas que hoy en día son muy relevantes y los riesgos que tendría su paralización o la perturbación de su funcionamiento. Así como también, se mencionarán ataques relevantes que han tenido lugar en infraestructuras críticas, las consecuencias que se han derivado y cómo se podrían haber evitado.

Más adelante, nos adentraremos en el mundo de la regulación específica en esta materia que se ha definido desde hace años y que ha ayudado a crear un marco regulatorio específico en este país. Empezaremos definiendo una infraestructura crítica y por qué está considerada como tal, para continuar con los riesgos y amenazas que se ciernen sobre algunas, con algunos ejemplos famosos que han ocurrido en este siglo y en el anterior.

Posteriormente, profundizaremos sobre el mundo PIC, la Ley PIC, y los diferentes organismos públicos que se han creado a raíz de la Ley y también los planes y medidas que se han definido en esta materia (PSO y PPE). Para, finalmente, desarrollar una serie de recomendaciones sobre la metodología de análisis de riesgos y las medidas de seguridad a implantar, de cara a profundizar lo indicado en los PPE y PSO para garantizar el funcionamiento de los servicios esenciales prestados por sus infraestructuras críticas.

2 Estado del arte

Actualmente, el mundo de las infraestructuras críticas está agrupado por sectores dependiendo del servicio que presten: administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y transporte[4].

Si bien, hace no muchos años, los Estados se defendían de los ataques mediante ejércitos, hoy en día, hay que tener en cuenta otras muchas variantes y tipologías de ataques. Es decir, las centrales nucleares, las centrales eólicas, solares, de agua, etc. que proporcionan energía a la población, y considerado, por tanto, un servicio básico a la ciudadanía, son claros objetivos de ciberataques dada su criticidad como infraestructura que presta un servicio esencial.
Cualquier ataque que suponga una perturbación o paralización sobre estas infraestructuras tendría unas repercusiones gravísimas sobre el estado de bienestar de cualquier país, ya que provocaría graves daños si la paralización de este tipo de servicios se llevara a cabo sobre un elevado porcentaje de centrales que presten este tipo de servicio.
También, existen otro tipo de infraestructuras críticas como las pertenecientes al sector de transporte, es decir, los aviones, los barcos, los trenes, etc. En este sentido, quizás no seamos conscientes de la dependencia actual del ser humano con respecto a los transportes que utiliza a diario, pero un fallo grave, mediante paralización del servicio, de un transporte como el avión, la red de metro de una gran ciudad, sobre todo en hora punta, donde multitud de personas se encuentran en estos puntos, puede suponer una catástrofe con elevado impacto en el estado de bienestar.
Todas estas infraestructuras hay que considerar que generalmente están conectadas a Internet de alguna manera por lo que siempre existe una posibilidad de ciber-ataque sobre sus instalaciones. Y dada la gran inversión que hay que realizar en materia de seguridad para conseguir una buena defensa ante este tipo de ciberataques, no es difícil para los hackers descubrir estas puertas de acceso a través de vulnerabilidades.
Si bien es cierto que hoy en día, algunas infraestructuras críticas como las centrales nucleares se están empezando a configurar para que se encuentren totalmente aisladas del exterior, es decir, que no exista ningún tipo de conexión a Internet.

Como ejemplo de ciber-ataque, no hace muchos años, ocurrió sobre una central nuclear en Irán provocando una alteración grave en su funcionamiento, no prestando su servicio normal, ya que consiguió paralizar muchas de sus máquinas, más de 45.000 sistemas de carácter crítico[5]. Si bien, esto finalmente fue detectado, el daño provocado podría haber sido mucho mayor si el hacker así lo hubiera querido. Y la puerta que comentábamos radicaba en sus sistemas informáticos y es que no se encontraban debidamente actualizados. Lo que supuso que el virus introducido pudiera buscar una vulnerabilidad a través del sistema operativo, lo que provocó que se adentrase en la red de manera bastante sencilla, modificando una librería .DLL de la aplicación WinCC (aplicación SCADA, dispositivo utilizado para el control y monitorización en entornos industriales). Este ataque se podría haber evitado realizando actualizaciones periódicas de los sistemas según suelen indicar los fabricantes, así como también si hubieran tenido una adecuada segregación de redes (diferentes redes y subredes, y zonas desmilitarizadas). Consiguiendo de esta forma,

[5] Noticia publicada por el diario digital BBC en septiembre de 2010.

que, una vez atravesada la "puerta" de un equipo del sistema, no viera o tuviera acceso a toda la red.
Por otra parte, también cabe indicar que estas medidas de seguridad propuestas se englobarían dentro de una serie de protocolos de seguridad y cumplimiento de normativas ISO/IEC 27000 que este tipo de infraestructuras críticas deberían de asegurarse y exigirse cumplir. Como, por ejemplo, una de ellas que es relativa a las verificaciones de integridad, y es que otra forma de haber evitado el ataque hubiera sido seguir una de esas normativas que comentábamos. Es decir, si se hubiera poseído un verificador de integridad con alertas e incluso con acciones o alarmas de mitigación automática, se habrían identificado las vulnerabilidades antes de que ocurriera el ataque, y éstas se podrían haber subsanado.

Otro ciber-ataque que tuvo lugar en octubre de 2016, a gran escala sobre un servidor de nombres, DNS, utilizado para asignar la correcta dirección a los nombres de las webs que el usuario inserta en su buscador. El ataque fue realizado mediante denegación de servicio distribuido, DDOS, sobre una empresa, Dyn, dedicada a prestar este tipo de servicio. El ataque se ejecutó utilizando dispositivos cotidianos conectados a Internet, realizando desde cada uno de ellos peticiones contra este DNS hasta colapsar sus colas de mensajes. Este ciber-ataque tuvo un especial impacto en la sociedad debido a que esta empresa presta servicio a empresas tan conocidas como Twitter, Spotify o Netflix.
Las dos ventajas que supo aprovechar el hacker fueron:

- Miles de personas que tienen en sus hogares dispositivos cotidianos, pertenecientes a una empresa china, con acceso a Internet (routers, grabadores digitales, cámaras) pero con contraseñas de configuración de seguridad muy débiles por defecto, y que además seguramente el hacker tuvo acceso a ellas;
- Y, por otra parte, que la mayoría de las personas que utilizaba este tipo de dispositivos no había cambiado la configuración de seguridad que viene por defecto.

Por tanto, el hacker se aprovechó de la ignorancia de las personas y las malas prácticas de la empresa china, para acceder a todos estos dispositivos y utilizarlos para su propio interés: lanzar tres ataques coordinados y planificados de peticiones de mensajes desde millones de dispositivos periféricos cotidianos, provocando el colapso y, por tanto, la suspensión del servicio de DNS que prestaba la empresa Dyn.
Las medidas que se podían haber implantado para evitar el ataque radican primero en la empresa china y su política de configuración de contraseñas, la cual se debería de fortalecer; así como una concienciación ciudadana acerca de fortalecer la seguridad de sus dispositivos domésticos que estén conectados a Internet.

3 La Infraestructura Crítica

Para que una infraestructura sea considerada crítica y forme parte del Catálogo Nacional de Infraestructuras Estratégicas deberá cumplir uno o varios de los criterios de criticidad pre-definidos en la Ley PIC, los cuales tienen que ver con las consecuencias que tendría un ataque sobre la infraestructura en términos de mal funcionamiento, destrucción o perturbación:

- El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.
- El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.
- El impacto medio ambiental, teniendo en cuenta la degradación en el lugar y sus alrededores.
- El impacto público y social, el sufrimiento físico y la alteración de la vida cotidiana.

El Catálogo Nacional de Infraestructuras Estratégicas contiene la información relativa a cada infraestructura crítica definida e identificada. Y el objetivo de esta recopilación de información es el de diseñar los mecanismos de planificación, prevención, protección y reacción ante eventuales ciber-amenazas, proporcionando así una rápida respuesta acorde a las características y criticidad de la infraestructura crítica amenazada. Este Catálogo también deberá contener cierta información administrativa de cada infraestructura crítica: titular, quién la gestiona, ubicación, servicio que presta, nivel de seguridad que necesita, etc.
Este Catálogo, dada la relevancia y criticidad de la información que contiene, está considerado como SECRETO y depende directamente del Ministerio del Interior.

Teniendo en cuenta las características anteriormente comentadas que debe cumplir la infraestructura para entrar a formar parte del Catálogo Nacional de Infraestructuras Críticas, a continuación, se mencionan algunos ejemplos razonados:

3.1 Algunas infraestructuras críticas

3.1.1 Presa de agua

Esta infraestructura destaca porque, en el caso de sufriera un ataque y su funcionamiento se viera afectado bien por destrucción o mal funcionamiento, tendría un fuerte impacto sobre el medio ambiente, así como también en el número de personas afectadas en términos de salud pública. Ya que un mal funcionamiento de la presa, podría, por una parte, tener como consecuencias el no abastecimiento de agua a pueblos o ciudades, y, por otra, si toda el agua contenida en la presa se soltase cuando no es debido, podría tener graves consecuencias para los campos de cultivo que se nutren de ella y/o que estuviesen en las cercanías de su desagüe.

Como infraestructura que es una presa, dispone de software instalado para el control digital de las máquinas que controlan y monitorizan su funcionamiento. Y, como suele ser normal, este tipo de infraestructuras disponen de un control local pero también disponen de un control sobre la infraestructura, pero a nivel autonómico, provincial o por zonas geográficas, enviando información sobre el nivel de agua contenida en la presa, así como el caudal abierto, entre otros. Para el envío de esta información, es precisa una conexión a internet, la cual ya se considera una puerta de entrada para un ciber-ataque. Aunque esto puede ser minimizado cuando la seguridad de los sistemas informáticos y comunicaciones instalados en la presa se encuentren debidamente securizados. En este sentido, hacemos referencia a firewalls, actualizaciones de sistemas operativos y bases de datos, routers, etc.

Y, además, algunas de estas infraestructuras también incluyen el tratamiento del agua, aunque también pueden ser infraestructuras diferentes. Para el tratamiento del agua, se utiliza software específico para añadir las sustancias concretas y las cantidades específicas. Muchas veces, este software está controlado de forma remota desde instalaciones a kilómetros de distancia. Y para ello, se establecen comunicaciones vía Internet, instalando en muchos casos routers domésticos para proporcionar acceso a Internet y permitir las comunicaciones mencionadas. Esto ya supone un riesgo elevado no tener controlado este router con un firewall bien configurado. Por ejemplo, si se mantiene la contraseña por defecto que trae el router, es muy fácilmente accesible desde el punto de vista de un hacker ya que muchas de estas contraseñas por defecto están generadas mediante algoritmos perfectamente conocidos y accesibles.

De esta forma, tendríamos acceso al router, habiendo adivinado la contraseña (mediante algún método de descifrado conocido o simplemente mediante un ataque de fuerza bruta) y, por tanto, viendo todos los dispositivos conectados a este router y transmitiendo su información. Esto suele suceder ya que, en la mayoría de los casos, la red no está perfectamente segmentada y, si tienes acceso al dispositivo de entrada, se pueden ver todos los dispositivos que están conectados a ésta.

3.1.2 Central eléctrica

Aunque, hoy en día, este tipo de infraestructuras están extremadamente protegidas y siempre existen sistemas redundantes para tener disponibilidad en caso de fallo, las consecuencias, si tuviera lugar una perturbación o incluso destrucción, podrían ser fatales.

En este caso concreto, hablamos de muchas personas afectadas, dependiendo del número de personas abastecidas (pueblos o ciudades), impacto económico ya que se trata de un servicio esencial y, como tal, las empresas están obligadas a ofrecerlo, y en caso contrario, conllevarían multas millonarias. Pero, sobre todo, el impacto público y social que tendría dejar sin energía a ciudades o pueblos.

Hoy en día, cualquier ciudad no es capaz de funcionar sin energía, es decir, dependemos completamente del uso de ésta. Y, al igual que con las presas, este tipo de infraestructuras están repartidas por todo el territorio nacional y, para su control, se utiliza software específico, SCADAs, que controlan y monitorizan las actividades de las diferentes plantas, enviando la información de éstas a las centrales de información.

Teniendo en cuenta esto, y como ya se demostrara en apartados anteriores, ya se han realizado ciberataques contra infraestructuras críticas que han logrado acceder a las máquinas, en este caso a las plantas de producción, y han parado su funcionamiento, aunque también han logrado que este ciber-ataque no fuera detectado por los sistemas de monitorización de la planta. Lo cual también es aplicable a las centrales eléctricas, es decir, un posible ciber-ataque sería encontrar una puerta trasera, un punto de acceso ya sea mediante un acceso forzado desde dentro como por ejemplo la conexión de un dispositivo usb infectado o un router no securizado adecuadamente. Y, una vez dentro, si la red no está segmentada correctamente, no utilizando por ejemplo *zonas desmilitarizadas*, ya tendríamos acceso a todos los dispositivos que estuvieran conectados a ella, pudiendo provocar el malfuncionamiento de estos o un uso no autorizado.

3.1.3 Aeropuertos

Hace no mucho tiempo, el FBI reveló que un avión de pasajeros[6], Boeing, estuvo pilotado por un hacker conocido durante un periodo de tiempo concreto no especificado. Este hacker consiguió elevar el avión de altura y sacar el avión de su rutina de vuelo. Esto es un ejemplo de vulnerabilidad que demuestra que los hackers hoy en día pueden aprovechar para el acceso y control de este tipo de transportes. Y es que probablemente este transporte sea uno de los más críticos y con mayor impacto social, así como también número de personas afectadas al mismo tiempo. Anualmente, tienen lugar millones de vuelos de pasajeros. Y una mínima perturbación o destrucción, como ya ha pasado en alguna ocasión, tiene las peores consecuencias que un desastre puede ocasionar. La mayor parte de los aviones están desarrollados para ser controlados y pilotados tanto de forma manual por los pilotos como de forma automática por el propio sistema informático y de navegación del propio avión. Esto significa que requiere de una conexión a internet hacia el exterior, lo cual supone ya una vía de entrada a cualquier hacker, en el caso de que los dispositivos implementados no estén adecuadamente securizados. Si bien, hoy en día, este tipo de transporte se encuentra especialmente vigilado contra ciber-ataques, la historia demuestra que son perfectamente "hackeables", pudiéndose adquirir el control del aparato y, por tanto, cabe la posibilidad de tener un accidente. Por ello, hay que hacer especial hincapié en este tipo de infraestructuras críticas y, en su seguridad, debido a su alto impacto en la sociedad.

3.1.4 Bancos

El mundo actual se mueve por sistemas monetarios dependiendo de la región geográfica. Esto significa que las sociedades civilizadas están perfectamente desarrolladas en base a los movimientos de dinero, compra y venta de recursos, salarios, etc. Para la orquestación de estos grandes movimientos de dinero, existen diferentes organismos, tanto los fabricantes de dinero como los grandes prestamistas e inversores, entre ellos los bancos. Hoy en día, nadie se imagina un mundo sin bancos. Estos son utilizados por el ser humano de forma cotidiana. Qué

[6] Noticia del periódico digital CNN del día 18 de mayo de 2015.

ocurriría si un día, los principales bancos de nuestro país se quedasen bloqueados… Existen casos similares que ya han ocurrido como en Argentina con el "corralito". Esto puede llegar a crear situaciones de verdadero pánico en la sociedad ya que no podríamos vivir sin dinero: la comida, las medicinas, la ropa, el transporte, etc.

Es por esto que los bancos están extremadamente regulados y se les exigen constantemente evaluaciones y actualizaciones de seguridad para asegurar el bienestar social.

En el caso de ciberataques sobre bancos, como ocurriera hace poco[7], en el que hackers consiguieron acceder al software de los cajeros y expulsar multitud de billetes de dinero de forma fraudulenta y remota, tiene obviamente un gran impacto social, económico y también sobre un gran número de personas afectadas.

[7] Noticia del periódico digital El País del día 23 noviembre 2016.

4 Evolución histórica de la seguridad para las infraestructuras críticas a nivel regulatorio

En España, el proceso de implantación de una metodología de seguridad para la protección de las infraestructuras críticas ha seguido cronológicamente una serie de fases:

- En 2007, La Secretaría de Estado de Seguridad del Ministerio del Interior aprobó el Plan Nacional para la Protección de las Infraestructuras Críticas. También, aunque posteriormente, los organismos públicos y privados adoptaron un acuerdo a gran escala en materia de Protección de Infraestructuras Críticas. Y, por último, en este año, se crea el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)[4].
- En 2011, se promulga la ley 8/2011, en concreto, el 28 de abril, a través de la cual quedan definidas y establecidas las medidas para la protección de infraestructuras críticas (*conocida como Ley PIC*). Y, posteriormente, se publica el Real Decreto 704/2011, el 20 de mayo, por el que queda aprobado el reglamento que desarrolla la ley (*RDPIC*).
- Entre 2011 y 2012, al haberse definido ya las medidas de seguridad, éstas fueron publicadas como Guías de contenidos mínimos y de buenas prácticas. Las cuáles deberían ser seguidas por los Operadores Críticos, de cara a la implantación de la Ley PIC[8].

  Ya, durante 2012, se firmó el Convenio Marco de Colaboración en materia de Ciberseguridad entre la SES (*Secretaría de Estado de Seguridad*) y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, con el objetivo de afrontar las ciber-amenazas.

  Teniendo en cuenta todo lo anterior, quedaba definido así la línea a seguir entre las entidades públicas y privadas, así como los objetivos a conseguir; entre ellos, una seguridad integral de las infraestructuras críticas. Asegurando de esta manera la protección de la sociedad y sus ciudadanos.
- En 2013, se iniciaron los estudios para la elaboración de los primeros Planes Estratégicos Sectoriales (PES). Esto fue llevado a cabo mediante la constitución de grupos de trabajo multidisciplinares bajo la coordinación del CNPIC. En este primer paso, fueron abordados los siguientes sectores:
  - Energético (electricidad, gas y petróleo)
  - Nuclear
  - Financiero
- También, en 2013, la Estrategia de Seguridad Nacional reconoce las ciber-amenazas como uno de los riesgos y amenazas a la seguridad nacional. Adicionalmente, el Esquema de Seguridad Nacional completa este enfoque con la apuesta específica por la protección en los sistemas de control industrial[9].

[8] Revista del Ministerio del Interior – Seguridad y Ciudadanía – 2014.

[9] Revista del Ministerio del Interior – Seguridad y Ciudadanía – 2015.

- En 2014, se finaliza la elaboración de los 5 primeros Planes de Seguridad del Operador (Electricidad, Gas, Petróleo, nuclear y financiero), bajo la supervisión de la Comisión Nacional PIC. Además, fueron también aprobados un total de 37 Operadores Críticos y, ya en 2015, los sectores: agua, transporte marítimo, aéreo, ferroviario y carretera. Y, en 2016, se han elaborado los Planes asociados a los sectores de la Industria Química y el Espacio, así como la designación de 11 nuevos operadores críticos[9].
- Actualmente, teniendo en cuenta los Planes Estratégicos Sectoriales ya definidos, están cubiertos 7 de los principales sectores de producción y un total de 106 Operadores Críticos ya asignados.
  Este hecho ha supuesto que, bajo las instrucciones y Guías del CNPIC, los Operadores Críticos hayan elaborado por primera vez sus propios Planes de Seguridad del Operador (PSO), así como también la elaboración de los Planes de Protección Específicos (PPE).
  La redacción de los PSO y PPE es obligación de los Operadores Críticos, así como también presentarlos, una vez terminados, a la autoridad competente para su aprobación, en este caso, el Secretario de Estado de Seguridad.

Adicionalmente, en 2006, en España, se crea un organismo especializado en los incidentes informáticos: CERT (*por sus siglas en inglés Computer Emergency Response Team*), el cual se convierte en un referente para los Operadores Críticos. Su principal atributo es la capacidad de respuesta a ciber-incidentes de seguridad de la información, formando parte del Ministerio de Energía, Turismo y Agenda Digital y del Ministerio del Interior.
En concreto, y por acuerdo del Consejo Nacional de Ciberseguridad, el CERTSI pasa a ser el CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas.
Esto significa que el CERTSI se convierte en el punto de referencia para los operadores de infraestructuras críticas para la resolución técnica de incidentes de ciberseguridad que puedan afectar a la prestación de sus servicios esenciales.
Este organismo está coordinado por el Centro Nacional de Ciberseguridad (INCIBE) y por el CNPIC.
El servicio que ofrece es 24x7 a los OCs, asegurando además una confidencialidad en la información tratada con los OCs mediante contratos de confidencialidad. Este organismo proporciona hojas de referencia, guías de securización y documentos de mejores prácticas a los OCs, en los cuales se demuestra su experiencia en la investigación de amenazas y gestión de incidentes, facilitando a los OCs el estudio y conocimiento para mejorar la protección de las infraestructuras críticas de sus organizaciones.

A nivel europeo, el proceso de formalización de estándares de seguridad en materia de infraestructuras críticas comienza en 2004, cuando el Consejo Europeo insta a la Comisión Europea a diseñar y definir una estrategia global en esta materia. Y, a finales de ese mismo año, se adopta el primer acuerdo sobre protección de las infraestructuras críticas que contiene algunas propuestas sobre prevención, preparación y respuesta de Europa frente a atentados terroristas.
Después de esto, se consigue elaborar y aprobar el PEPIC, Programa Europeo de Protección de Infraestructuras Críticas. Adicionalmente, se pone en marcha también una red de información a través de alertas en infraestructuras críticas (*Critical Infraestructures Warning Information Network – CIWIN*).

Ya en 2008, con la entrada en vigor de la Directiva 2008/114, se define la responsabilidad de proteger las infraestructuras críticas europeas, la cual recae sobre los Estados miembros y los operadores de las mismas.

5 Esquema Nacional de Seguridad

Cuando la Ley PIC fue aprobada, se puso de manifiesto la importancia que tenía la seguridad de las infraestructuras críticas como parte de la Seguridad del Estado.
Y, de entre todos los sectores establecidos en este país, el sector industrial es uno de los más relevantes y también más críticos por los servicios esenciales que presta. Por lo que se creó específicamente el Esquema Nacional de Seguridad (*ENSI*).
El ENSI surge como elemento homogeneizador para todas las organizaciones de este sector ayudándoles a mejorar sus capacidades, minimizar los riesgos a los que se ven sometidos sus servicios esenciales y establecer metodologías y medidas para su mitigación, siendo este Esquema aplicable a cualquier sistema de control industrial.
Sus principios son:

- Ayudar a mejorar la seguridad de las organizaciones del sector industrial, garantizando la continuidad de los servicios prestados y cumplir las normas regulatorias
- Agilizar la adaptación a nuevos casos y sectores
- Buscar el entendimiento entre las empresas del sector de la ciber-seguridad y los Operadores Críticos del sector industrial.

En definitiva, el ENSI desarrolla una función integradora entre los OCs, los sistemas de control industrial y los organismos reguladores, de forma que el ENSI desarrolla procedimientos y herramientas en este ámbito para que los OCs puedan utilizarlos y parametrizarlos mejorando la seguridad de sus organizaciones.

Los objetivos perseguidos por el ENSI son:

- Ayudar a los OCs a mejorar la seguridad de sus sistemas de control industrial ante ciberataques.
- Mejorar la ciber-resiliencia de sus sistemas para elevar la capacidad de estos sistemas para soportar y recuperarse ante ciber-desastres y ciber-perturbaciones.
- Facilitar a los OCs la aplicación de la regulación de la ciber-seguridad sobre las infraestructuras críticas.
- Homogeneizar el tratamiento de la ciber-seguridad en entornos industriales.
- Mejorar la seguridad de la cadena de valor OC-Proveedor crítico.

Para dar cumplimiento a estos objetivos, el ENSI presenta sus 5 elementos esenciales:

- Política General: ésta define los objetivos, los requisitos para cumplir los objetivos y los beneficios que se esperan de la implantación del esquema de seguridad en el ámbito industrial. Identificando además a los actores y partes interesadas para su colaboración con el ENSI y conseguir de esta forma entre todos mejorar la ciber-seguridad en el entorno industrial.
- Metodología de Análisis de Riesgos Ligero de Ciber-Seguridad (*ARLI-CIB, modelo basado en guías y estándares internacionalmente reconocidos como ISA/IEC 62443 e ISO/IEC 27000*): este sistema proporciona a las organizaciones un modelo sencillo y práctico de análisis de riesgos sobre cualquier tipo de sistema de control

industrial. Estableciendo y facilitando a los Operadores Críticos modelos ya definidos para prevenir, identificar, analizar, evaluar y tratar a tiempo riesgos que afectan a infraestructuras que utilizan sistemas de control industrial. Además, se solicitará a los OCs que una vez realizados los análisis de riesgos utilizando este modelo, los resultados sean enviados de forma confidencial al ENSI para su investigación y análisis, ayudando de esta manera a la mejora y evolución en la ciber-seguridad industrial. Las diferentes fases de este análisis de riesgos son:
    - Identificación de los riesgos que pudieran afectar al sistema de control industrial del OC.
    - Estimación de la probabilidad de que dichos riesgos se materialicen.
    - Estimación del impacto en caso de producirse.
    - Tratamiento de los riesgos hasta que estos puedan asumirse.
- Indicadores para la Mejora de la Ciberresiliencia (*IMC*): Este modelo de indicadores permite medir el nivel de ciberresiliencia o capacidad de recuperarse a los sistemas de control industrial ante ciberataques, ciber amenazas o ciber-incidentes que puedan sufrir, permitiendo de esta forma anticipar, resistir, recuperar y evolucionar, mejorando de esta manera la capacidad de ciberresiliencia de su sistema de control industrial. Este modelo ya tiene asociada una herramienta diseñada para tal efecto que los OCs podrán utilizar y parametrizar según su propio negocio. Las fases de este modelo son:
    - Anticipación de la posibilidad de un incidente
    - Resistir durante la duración del incidente
    - Recuperación de la actividad una vez que el incidente ha tenido lugar y éste ha sido solucionado
    - Evolución de la organización para evitar que el incidente se repita en un futuro.
- Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor (*C4V*): Este modelo proporciona una herramienta para la evaluación del estado de madurez de los controles de una organización, así como de su cadena de valor, es decir, de sus proveedores, especialmente, los más críticos. Además, esta herramienta permite establecer unos valores mínimos aceptables en función de los resultados obtenidos en el análisis de riesgos realizado.
- Sistema de Acreditación en Ciberseguridad: Mediante este sistema, se busca:
    - Especificar un mínimo número de controles de ciberseguridad que deben estar implantados en los OCs y sus arquitecturas que controlan la prestación de los servicios esenciales.
    - Definir los métodos que permitan la evaluación de los controles implantados.
    - Desarrollar procedimientos, medios y mecanismos que permitan acreditar la implantación de los mínimos controles requeridos.
    - Finalmente, garantizar unos niveles mínimos equiparables entre todos los OCs que presten servicios análogos.

Según el ENSI, el primer paso para poner en práctica sus guías de actuación es la ejecución del análisis de riesgos de ciberseguridad. Este análisis permite que el OC mejore los conocimientos que tiene sobre sus operaciones, cómo se realizan éstas y sobre todo aquellos activos vitales utilizados para la prestación de los servicios esenciales. Para llevar a cabo dicho análisis, el ENSI proponer aplicar el ARLI-CIB. Y, tras este análisis de riesgos, las otras utilidades proporcionadas por el ENSI pueden ser aplicadas, mejorando así la capacidad de ciber-resiliencia de la organización.

6 Plan de Seguridad del Operador

6.1 Introducción

Según el artículo 13 de la Ley 8/2011, se establece la obligación que tienen los Operadores Críticos de elaborar Planes específicos relativos a la seguridad de sus infraestructuras críticas con además una serie de contenidos mínimos que estos Planes deben incluir. Dichos Planes son el Plan de Seguridad del Operador (*PSO*) y el Plan de Protección Específico (*PPE*).
Por tanto, el objetivo de este apartado es de servir de guía a los Operadores Críticos mediante unos contenidos mínimos en el diseño y elaboración de un Plan de Seguridad del Operador.

El objetivo principal del PSO es el de definir la política general del Operador que garantice la seguridad integral (*tanto seguridad física como ciber-seguridad*) en los activos y estructura que soporta la infraestructura crítica, incluyendo los sistemas de información y las instalaciones.
Esta política deberá contener, al menos, información sobre los siguientes aspectos:

- Política general de seguridad del Operador Crítico y marco de gobierno
- Los servicios esenciales prestados por el Operador Crítico
- Metodología de Análisis de riesgos
- Criterios de aplicación de las Medidas de Seguridad Integral

Este documento, una vez realizado, deberá ser presentado al CNPIC (*Centro Nacional para la Protección de las Infraestructuras Críticas*) para su validación y aprobación.
Además, se les exige a los Operadores Críticos que realicen una revisión bienal de este documento. Y, en el caso de que, tras realizar la revisión, exista la necesidad de actualizar algún aspecto, el documento con las actualizaciones deberá ser enviado de nuevo al CNPIC para su validación y aprobación.
Por otra parte, cualquier tipo de modificación de las características de la infraestructura crítica, así como cualquier circunstancia que le pueda afectar, deberá ser incluido en el propio documento o como anexo, para su validación y aprobación por parte del CNPIC.

En relación a la información contenida en este tipo de documento, y según la Ley 8/2011, ésta se deberá tratar como información confidencial dado el valor estratégico de ésta para cualquier Compañía. En este sentido, los Operadores Críticos que sean propietarios o gestionen una infraestructura crítica y, por tanto, dispongan de un Plan de Seguridad del Operador, se deberán regir por las orientaciones en materia de protección de la información publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia, en lo que se refiere al manejo y custodia de información clasificada con grado de difusión limitada.

6.2 Política General de Seguridad y Marco de Gobierno

Una política de seguridad debe servir de soporte y guiar a cualquier empresa en la gestión de la seguridad. Para lo cual, la Dirección de la Compañía deberá estar fuertemente involucrada en el seguimiento y divulgación de la política, haciéndola cumplir en todo momento. Esta política de seguridad debe establecer las líneas base de la Organización para su actuación y compromiso de cumplimiento para con la seguridad.

A partir de esto, cada Operador Crítico deberá definir su propia política de seguridad muy orientada a las infraestructuras críticas y su protección. Además, teniendo que hacer de esta política un marco de referencia para el tratamiento de cualquier tipo de sus infraestructuras en materia de seguridad, para su protección.

Según la Ley ya mencionada, desde la Secretaría de Estado de Seguridad, a través del CNPIC, se establecen los contenidos mínimos que cada Operador Crítico deberá incluir en su política:

- Un objetivo claro, definido y consecuente con el negocio de la organización, las infraestructuras críticas de las que dispone y la seguridad de éstas.
- Dado que una política de seguridad puede no tener como alcance la totalidad de una Organización, cada Operador Crítico deberá detallar específicamente el alcance de la política, indicando a qué parte de la Organización contempla.
- Dada la importancia que tiene una política de seguridad para cualquier Organización, es de especial relevancia que la Dirección de la Organización apoye y dé ejemplo con su cumplimiento, bien sea a través de una persona o departamento, con la capacidad para poder implantar esta política en la Organización. De esta forma, los empleados percibirán un compromiso por parte de la Dirección, facilitando el cumplimiento.
- Esta política de seguridad deberá tener un carácter integral. Si bien es cierto que este documento se limita a la protección de las infraestructuras críticas por ciber-amenazas, todo software necesario para la protección de estas ciber-amenazas estará soportado por un hardware que también requiere de unas medidas de seguridad físicas aplicables. En este sentido, la política deberá definir las estrategias y líneas de actuación de la Organización en este ámbito, incorporando los recursos necesarios para hacerla cumplir.
- Al tratarse de un documento, éste deberá ser actualizado periódicamente. Cada Operador Crítico será responsable de mantener siempre actualizado este documento incluyendo cualquier cambio aplicable. Por tanto, se deberá establecer un procedimiento para la actualización de este documento, incluyendo responsables y fechas, así como aprobaciones. Además, será muy importante que este documento se mantenga actualizado en lo referente a las infraestructuras críticas del Operador Crítico en cuanto a amenazas, nuevas infraestructuras, modificaciones de éstas, salvaguardas, o cualquier aspecto que pueda tener impacto sobre la seguridad de las infraestructuras críticas del Operador.

Con respecto al Marco de Gobierno, la Organización deberá establecer una serie de requisitos en lo relativo a la gestión de la seguridad.

En primer lugar, en cuanto a la organización de la seguridad y comunicación, cada Operador Crítico deberá definir su propia estructura de seguridad a dos niveles: primero, la

estructura de seguridad corporativa y, después, con un mayor nivel de detalle, la estructura de seguridad donde se describan las funciones de los principales responsables, así como también las áreas de la Organización.

Como parte de la definición de estas estructuras, cada Operador Crítico deberá definir un Responsable de Seguridad y Enlace y a los sustitutos correspondientes, así como también a los Delegados de Seguridad para cada una de sus infraestructuras críticas. El OC deberá asegurarse que estas personas disponen de los conocimientos y certificaciones suficientes para desempeñar estos cargos. El Responsable de Seguridad y Enlace deberá estar habilitado por el Ministerio del Interior como Director de Seguridad o tener una habilitación equivalente. Sus datos personales de contacto deberán ser comunicados al CNPIC. Sus funciones serán las de representar al Operador Crítico ante la Secretaría de Estado de Seguridad en lo relativo a la seguridad de las infraestructuras críticas de su Organización, así como a los diferentes Planes elaborados por el OC. También, será la línea oficial de comunicación entre los organismos públicos como el CNPIC y el CERTSI y su Organización.
Por otra parte, también, el Operador Crítico deberá nombrar a un Delegado de Seguridad por infraestructura, así como sus sustitutos, detallando sus datos personales de contacto a los organismos competentes como el CNPIC. Tanto el Delegado como su sustituto deberán asegurar formación en seguridad y demostrarla ante los organismos. El nombramiento de estos deberá ser realizado en los plazos que estipula la Ley 8/2011. Las funciones de este responsable serán las de ejercer como canal de comunicación entre su Organización y las autoridades competentes en lo relativo a la seguridad de su infraestructura crítica, y también para trasladar las necesidades operativas de su infraestructura crítica a las autoridades competentes.

También, como parte de la estructura de seguridad a un mayor nivel de detalle, cada Operador Crítico deberá describir su organigrama de seguridad con las ubicaciones físicas de las principales instalaciones de la Organización, así como de sus infraestructuras críticas. Y, también, se deberán describir los Comités u órganos de decisión en materia de seguridad, así como las funciones de cada uno de ellos.

Por otra parte, y en el caso de que el Operador tenga servicios contratados con proveedores externos, subcontratados, estas relaciones se deberán incluir en los organigramas y en las estructuras de seguridad, describiendo exactamente el tipo de servicio externalizado, a qué proveedores, el periodo, los controles establecidos para la monitorización del cumplimiento del contrato, y las sedes de estos proveedores.

En lo relativo a la ciber-seguridad y su protección en las infraestructuras críticas, será el CERT de Seguridad e Industria el responsable de la resolución de las incidencias cibernéticas que puedan afectar a la seguridad de las infraestructuras críticas de los OC. En este sentido, será el CERTSI el órgano que trabaje conjuntamente con el CNPIC para el estudio, detección, análisis, aviso y evaluación de ciber-amenazas para con los Operadores Críticos. Estudiando y estando alerta ante posibles ciber-ataques y en constante comunicación con los Operadores Críticos.

Una parte muy importante de la Política de Seguridad y del Marco de Gobierno será la relativa a la formación específica en materia de seguridad para la protección de las infraestructuras críticas. Cada Operador Crítico deberá describir sus planes de formación indicando las actividades a realizar, los periodos, los mecanismos de evaluación y las

personas afectadas. Así como también, registros que demuestren que su práctica se ha llevado a cabo. Todo esto deberá estar recogido en un Plan de Formación del Operador Crítico. Los principales aspectos en los que se deberá formar son:

- Seguridad integral
- Autoprotección
- Seguridad sobre el medio ambiente
- Habilidades organizativas y de comunicación
- Responsabilidades y actividades en caso de materializarse un incidente o en el caso de que se active un Nivel 4 o 5 de amenaza del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

Como parte de esta formación, cada Operador Crítico deberá realizar periódicamente ejercicios de simulación de ciber-ataques sobre sus infraestructuras críticas, estudiando previamente las amenazas a utilizar para explotar las vulnerabilidades de sus infraestructuras críticas y así poder evaluar la confiabilidad de sus controles implementados sobre éstas.

Finalmente, toda esta gestión de la seguridad integral deberá estar soportada sobre un Modelo de Gestión Aplicado, en el cual se recoja en cada momento la situación de exposición de la Organización. En este sentido, cada Operador Crítico deberá establecer un sistema, que se encuentre actualizado, donde se recojan sus infraestructuras críticas, los riesgos identificados y asociados a éstas, los controles implementados y el nivel de exposición restante en función del incidente materializado y su nivel de actuación. Además, teniendo en cuenta esto, este modelo deberá aplicar por sí mismo las medidas de seguridad existentes en la Organización, así como activar los mecanismos de seguridad existentes implantados.
Y la mejor forma de implementar este modelo de gestión será un sistema informático que esté conectado con los sistemas que soportan las infraestructuras críticas de tal forma que éstas se encuentren siempre monitorizadas, así como su seguridad. Y, en el caso de materializarse algún incidente, deberá ser detectado por el Modelo que activará los mecanismos de seguridad apropiados al incidente.

Por último, se deberán establecer las comunicaciones con el CNPIC en los casos en los que un incidente o situación pueda poner en riesgo la seguridad de alguna infraestructura crítica, utilizando el protocolo de comunicación previamente establecido con el CNPIC.
Y, en lo relativo a los ciber-incidentes, las comunicaciones serán realizadas con el CERTSI, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior.

6.3 Servicios prestados por el Operador Crítico

Desde el CNPIC, se les exige a los Operadores Críticos que incluyan en el Plan de Seguridad del Operador un resumen de ciertos aspectos generales de su Organización.

En primer lugar, el OC deberá describir los servicios prestados por su Organización haciendo especial mención a aquellos que sean esenciales para la ciudadanía (*funciones sociales básicas: la salud, la seguridad, el bienestar social y económico; el adecuado funcionamiento de las Instituciones del Estado y Administraciones Públicas*). Los cuáles sean prestados a través de sus infraestructuras críticas.

Por otra parte, cada Operador Crítico deberá revisar bianualmente la relación de sus servicios prestados de cara a la posible actualización o modificación del contenido del Plan de Seguridad del Operador.

También, como parte del contenido del PSO, cada OC deberá incluir un estudio de las consecuencias de la interrupción de sus servicios esenciales prestados. En este sentido, cada OC deberá describir, en función de sus servicios esenciales, las consecuencias de una alteración o perturbación de su funcionamiento o también de su posible destrucción. Incluyendo en este estudio, el alcance de recursos afectados, ya sean seres humanos, medio ambiente, etc. Y también deberán incluir los servicios y/o operadores dependientes que pueden haberse visto afectados por un incidente de los comentados.
Y, en el caso de que este incidente tenga lugar, qué alternativas puede prestar el propio operador u otros al servicio afectado, así como los tiempos esperados de recuperación y nivel del servicio restaurado.

6.4 Metodología de análisis de riesgos

Cada Operador Crítico deberá incluir en su PSO la metodología de análisis de riesgos empleada. Este análisis de riesgos deberá contemplar la totalidad de las amenazas que puedan afectar a los activos que componen las infraestructuras críticas del Operador, así como garantizar la continuidad de los servicios prestados por éste. Estableciendo en cada caso las salvaguardas y controles necesarios para mitigar los impactos de la materialización de esas amenazas.

Además, como parte del análisis de riesgos, el Operador Crítico deberá hacer mención a las interdependencias que tenga con otros servicios prestados por otros operadores, ya sea del mismo sector o de otros, y también si existen con operadores de otros países. Por último, también incluir, si existen, dependencias con los proveedores de algún tipo de servicio dentro de la cadena de suministros y con aquellos que proporcionan servicios TIC, como proveedores de telecomunicaciones, de hardware, housing, etc.
Para cada uno de ellos, se deberá incluir un detalle de los Acuerdos de Nivel de Servicio contratados.

Con respecto a la metodología de análisis de riesgos, se deberá incluir en el PSO en líneas generales el diseño de ésta, de tal forma que sirva de guía para la ejecución del análisis de riesgos en cada Plan de Protección Específico por cada infraestructura crítica. En este sentido, al menos, se deberán incluir los siguientes aspectos:

- Las etapas principales del análisis de riesgos a llevar a cabo sobre cada infraestructura crítica.
- Los algoritmos de cálculo aplicados en el análisis de riesgos como por ejemplo en el cálculo del nivel de impacto, riesgo residual o inherente.

Una parte muy importante del análisis de riesgos será la descripción de los recursos disponibles que soportan cada infraestructura crítica. Ya que, a partir de ellos, y las posibles amenazas, se identificarán los riesgos y las vulnerabilidades.
Como activos, se pueden destacar aquellos recursos necesarios para que la Organización funcione correctamente y, en especial, las infraestructuras críticas. Estos recursos se pueden clasificar en:

- Personas
- Sistemas informáticos
- Redes de comunicaciones
- Instalaciones necesarias para su operación

En cuanto a las amenazas, los Operadores Críticos deberán utilizar el árbol de amenazas ya diseñado por el CNPIC. A partir de cual, podrán concretar y especificar algunas de ellas, modificando sus características, así como también eliminar o añadir nuevas.
También, deberán hacer distinción entre aquellas amenazas intencionadas que pueden afectar a las infraestructuras críticas de las procedentes de interdependencias.

Y, por último, como el resultado del análisis de riesgos, cada OC deberá incluir en el PSO las líneas generales para la realización de la valoración de riesgos, identificando las categorías de clasificación de los riesgos, la metodología de mitigación (*reducción, eliminación, externalización, etc.*), mecanismos a implementar y activar en caso de reducción del riesgo, y, muy importante, descripción de los mecanismos que se activarán y cómo serán tratados los riesgos para aquellas amenazas con baja probabilidad pero alto impacto.

Este proceso de análisis y valoración de riesgos deberá ser realizado con cierta frecuencia dejando siempre constancia mediante registros o evidencias de su realización, supervisión y aprobación.

6.5 Criterios de aplicación de las medidas de seguridad

En líneas generales, cada Operador Crítico deberá mencionar las medidas de seguridad implantadas sobre los activos que componen las infraestructuras críticas como resultado del análisis de riesgos realizado para hacer frente a las amenazas identificadas. Esto servirá de guía para su mayor detalle en cada Plan de Protección Específico por cada infraestructura, donde se detallarán las medidas de seguridad implantadas.

6.6 Normativa, buenas prácticas y regulatoria

El Operador Crítico deberá recoger en una breve referencia la normativa relativa a:

- Seguridad física
- Ciber-seguridad
- Seguridad de la información
- Seguridad personal
- Seguridad ambiental
- Autoprotección y Prevención de Riesgos Laborales

7 Plan de Protección Específico

7.1 Introducción

Con la aprobación de la Ley 8/2011, se establecieron una serie de obligaciones y requisitos mínimos que todo Operador Crítico debe cumplir en cuanto a la elaboración de Planes de seguridad se refiere. En este sentido, en concreto, esta Ley exigía a cada Operador Crítico, que fuera propietario o gestor de una infraestructura crítica, la elaboración de un Plan de Protección Específico por cada infraestructura crítica. Además, la elaboración de este Plan no es libre, sino que, desde el CNPIC, se establecieron unas bases mínimas en cuanto a contenido que debían cumplir.

Por tanto, el objetivo de este apartado es de servir de guía a los Operadores Críticos en el diseño y elaboración de un Plan de Seguridad del Operador.

Si bien es cierto que, según esta Ley, cada Operador Crítico debe elaborar un Plan de Seguridad del Operador (PSO) y, a su vez, por cada infraestructura crítica, un Plan de Protección Específico (PPE); los PPE estos deben estar alineados con los PSO de cada Operador Crítico (OC), dado que este último se trata de un Plan a más alto nivel, el cual debe contener las líneas generales de actuación de cada OC y sus infraestructuras críticas, y contener todos los PPE definidos y asociados.

Un PPE es un documento operativo por infraestructura crítica donde quedan definidas las medidas de seguridad a aplicar por cada OC en cada infraestructura crítica para asegurar la seguridad integral (tanto física como la relativa a la ciber-seguridad) de ésta.

Todos los PPE deberán ser revisados con una frecuencia bienal y esta revisión y sus resultados deberán ser comunicados y aprobados por los organismos públicos competentes en este ámbito, entre ellos el CNPIC. Así, de esta forma, cualquier actualización o modificación, también deberá ser aprobado por estos organismos públicos. Todas estas actuaciones deberán quedar registradas: los responsables de su aprobación, las fechas en las que se aprueban las actualizaciones o modificaciones, las notas, documentos generados a posteriori, etc.

7.2 Política de Seguridad

El primer requisito que debe contener cada PPE es una política de seguridad aplicable al OC y a la infraestructura crítica definida en el PPE. Esta política debe contener un diagrama de la estructura funcional donde queden definidas las personas responsables, sus roles definidos y la jerarquía establecida en la toma de decisiones (*serán de aplicación todas aquellas personas con algún tipo de responsabilidad o impacto sobre la seguridad de la infraestructura crítica en cuestión o con impacto en ella*). Teniendo en cuenta que cada OC puede disponer de más de una infraestructura crítica y también cada OC puede disponer otros Planes, como el de Contingencia, Director de Seguridad, etc., deberá existir una relación definida para este tipo de dependencias conteniendo cualquiera que pueda existir entre la infraestructura crítica y otras infraestructuras críticas o con otros Planes.

Por otra parte, cada PPE deberá definir la figura del Delegado de Seguridad, así como su sustituto, indicando, además, los detalles personales de contacto de estas personas. Una vez definidos, así como cualquier cambio que tenga lugar sobre estos, deberán ser comunicados a la mayor brevedad posible al CNPIC y al resto de organismos públicos aplicables. Estas personas incluidas como Delegado de Seguridad deberán haber cumplido la formación establecida y exigida en el Plan de Formación del PSO.

Con respecto a los mecanismos de coordinación, desde el CNPIC, se exige que cada PPE establezca los mecanismos de coordinación necesarios para asegurar la seguridad de la infraestructura crítica afectada entre el Delegado de Seguridad definido en este documento y el Responsable de Seguridad y Enlace definido en el PSO, y, también, la coordinación entre estos y las autoridades competentes (*como por ejemplo las Fuerzas y Cuerpos de Seguridad del Estado*). Por último, cada PPE deberá contener también los mecanismos de coordinación con ciertos organismos públicos específicos en el ámbito de la seguridad, como son el CERT de Seguridad e Industria, así como los proveedores del OC definidos como críticos por su impacto sobre el servicio que presta la infraestructura en cuestión.

7.3 Descripción de la infraestructura crítica

El CNPIC exige que el Operador Crítico incluya cierta información específica sobre cada infraestructura crítica en cada PPE correspondiente.
En primer lugar, deberá contener información general relativa a la propia infraestructura como el tipo de instalación, el servicio que proporciona, cómo se realiza la gestión de la misma, su ubicación o ubicaciones físicas, los activos que la componen, la estructura de la misma, los sistemas de información que la soportan y su arquitectura, a quién presta servicio (*otras compañías, poblaciones, etc.*), relaciones y dependencias con otras infraestructuras tanto si son necesarias o no para la prestación del servicio esencial.

Por otra parte, hay que hablar de los activos y/o elementos de la infraestructura crítica que el PPE debe incluir. En concreto los activos, esenciales y no esenciales que soportan la infraestructura. Como activos se entienden:

- Las instalaciones y los componentes que son esenciales y necesarios para la prestación del servicio esencial que presta la infraestructura crítica.
- Los sistemas informáticos (*tanto hardware como software*) que soportan la infraestructura, tanto para la gestión del servicio esencial como la monitorización del servicio y la propia infraestructura, indicando todo el detalle posible acerca de estos.
- Las redes de comunicaciones: indicando las arquitecturas implementadas, los componentes utilizados, etc.
- Las personas involucradas en la gestión del servicio esencial prestado por la infraestructura crítica, tanto para la explotación del propio servicio, la seguridad de la infraestructura, etc.
- Los proveedores asociados al servicio prestado por la infraestructura crítica y, por tanto, considerados como críticos y esenciales. Teniendo, además, que incluir las medidas de seguridad pactadas con los proveedores en caso de que estos fallen en la prestación de su servicio y las acciones que se tendrían que llevar a cabo en ese caso, ya sean con ellos o con otros. Se incluyen proveedores de comunicaciones, electricidad, etc.

Y, por último, son muy relevantes las interdependencias del servicio que presta la infraestructura crítica y la propia infraestructura con otros entes. En este sentido, será muy importante que quede bien definido, en el PPE, la realidad de posibles dependencias con:

- Otras infraestructuras críticas del propio OC.
- Otras infraestructuras estratégicas del propio OC.

- Otras infraestructuras de otros OC
- Otros servicios de otros OC
- Los proveedores de servicios de la infraestructura crítica del OC

Como ya se comentaba anteriormente, este apartado es especialmente relevante por el impacto que puede tener una perturbación en alguna de las dependencias y las consecuencias que esto puede conllevar.
Por ejemplo, toda dependencia con un proveedor de comunicaciones será muy crítica, así como con el proveedor de electricidad. Debido a los sistemas de información que soportan la infraestructura necesitan su conexión a Internet para estar monitorizados y poder transmitir cualquier error identificado.

7.4 Protección y Gestión de la información y documentación

Teniendo en cuenta la información generada y contenida en cada PPE, se trata de información altamente sensible y confidencial por contener información crítica de cada infraestructura crítica, la cual debe estar especialmente protegida. Dado que, si esta información es sustraída, puede ser utilizada para atacar de forma específica y más dañina la infraestructura crítica dado que serías capaz de averiguar los puntos débiles, resultados de los análisis de riesgos, vulnerabilidades, etc.
Por tanto, se deberán establecer procedimientos específicos y formales para la protección y salvaguarda de esta documentación generada, asegurando además una clasificación apropiada según la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia, en lo que se refiere a manejo y custodia de información clasificada.

También, no hay que olvidar que será muy importante disponer de copias de los documentos, almacenados apropiadamente, ya que, al tratarse de procedimientos operativos, en caso de pérdida o destrucción, poder acceder siempre a la información, asegurando, por tanto, que estos documentos se encuentren almacenados tanto en digital como físico en lugares diferentes.

7.5 Metodología de Análisis de Riesgos

Esta Ley exige que cada PPE incluya la definición de una metodología de análisis de riesgos para su infraestructura crítica que asegure el funcionamiento de los servicios proporcionados por ésta.

En este sentido, se deberán tener en cuenta las amenazas con impacto posible en la infraestructura, teniendo en especial consideración aquellas con baja probabilidad de ocurrencia, pero elevado impacto. Considerando, en todos los casos de amenazas, la materialización de éstas y sus consecuencias en el servicio proporcionado por la infraestructura crítica, ya sea su destrucción o perturbación. Estas amenazas deberán ser clasificadas según su origen y objetivo, teniendo que incluir al menos las siguientes:

- Aquellas amenazas cuyo objetivo sea directamente la infraestructura

- Aquellas cuyo objetivo sean las interdependencias con otros activos o infraestructuras.
- Aquellas cuyo objetivo sean los sistemas informáticos que soportan la infraestructura y gestionan el servicio prestado por ésta.
- Y también aquellas amenazas que afectan sobre los activos de la infraestructura dedicados a la seguridad de ésta.

El CNPIC ha elaborado un árbol de amenazas, el cual deberá ser tenido en consideración, especialmente aquellas amenazas de origen terrorista o intencionado.
Indicar que este análisis de riesgos deberá tener en cuenta a la hora de clasificar las amenazas, los niveles definidos en el Plan de Prevención y Protección Antiterrorista y el Plan Nacional de Protección de Infraestructuras Críticas, los cuales ya recogen una serie de amenazas establecidas y clasificadas.

Y, como resultado del análisis de riesgos, para cada par activo/amenaza identificado y asociado, se establecerá la valoración de riesgos a partir de la metodología de análisis de riesgos especificada en el PSO del OC. Debiendo incluirse como mínimo los siguientes aspectos:

- Quién ha evaluado y aprobado el riesgo y su plan de mitigación
- Criterios de valoración del riesgo utilizados
- Fecha del último análisis de riesgos realizado sobre el par activo/amenaza
- Resultado de la valoración de riesgos en cuanto al nivel de riesgo aceptado

Comentar que todos aquellos riesgos aceptados y no mitigados deberán ser comunicados al CNPIC para su validación, sobre todo aquellos con alto nivel de impacto y baja probabilidad de ocurrencia.

Por otra parte, si una vez realizado el análisis y la valoración de riesgos sobre los activos/amenazas y las medidas de seguridad ya implementadas, se llegase a la conclusión de la necesidad de implementar nuevas medidas de seguridad complementarias a las ya existentes, éstas se deberán describir y listar, incluyendo para cada una de ellas, el procedimiento de implementación, su operativa, qué par activo-amenaza sería afectado, en forma de planes de acción. Estos planes de acción con las nuevas medidas deberán ser comunicadas al CNPIC para su aprobación.

7.6 Medidas de seguridad

El análisis de riesgos ya comentado identificará las vulnerabilidades y los riesgos de la infraestructura crítica. A partir de aquí, se añadirán las medidas de seguridad integral existentes para la mitigación de los riesgos identificados (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación). Resultando de esta manera los planes de acción correspondientes.

Con respecto a las medidas de seguridad ya existentes, se deberán clasificar en permanentes, es decir, aquellas que se encuentran ya implementadas para la protección de la ciberseguridad de la infraestructura. También, hay que incluir aquellas que se implanten como resultado del análisis de riesgos ejecutado. Se entiende por éstas, aquellas que sean necesarias para mitigar riesgos que no están cubiertos y cuya materialización supondría un grave incidente para el servicio prestado por la infraestructura crítica.

Por otra parte, estarían las medidas de seguridad temporales o graduales. Son aquellas que se definen y se implantarían, pero sólo serían activadas bajo ciertas circunstancias, como pueden ser la activación de alguno de los niveles de seguridad establecidos respectivamente en el Plan Nacional de Protección de las Infraestructuras Críticas, en coordinación con el Plan de Prevención y Protección Antiterrorista, principalmente para los niveles 4 y 5. Aunque también se puede dar el caso de activación de este tipo de medidas debido a la comunicación de las autoridades competentes como consecuencia de una amenaza específica que pueda llegar a afectar a la infraestructura crítica y al servicio que presta.

Posteriormente, existen una serie de medidas, organizativas y operacionales y de protección, que el CNPIC recomienda y que cada Operador Crítico deberá de incluir al menos. Entre ellas, se encuentran:

- Organizativas: El análisis de riesgos y el organigrama (*con una asignación de responsabilidades bien definida*) ya comentados, un cuerpo normativo (*incluyendo las políticas, procedimientos y estándares de seguridad*), normas y regulaciones de aplicación, y certificaciones, acreditaciones y evaluaciones de seguridad.
- Operacionales:
    - Se les exigirá a los OC disponer de un procedimiento que describa y defina el Ciclo de Vida de los activos que componen la infraestructura crítica.
    - También, se exigirá que hayan definido procedimientos para la formación y concienciación en materia de seguridad de la infraestructura crítica.
    - Procedimientos para la contingencia y recuperación en caso de perturbación o desastre.
    - Procedimientos para la monitorización, supervisión y evaluación del funcionamiento normal de la infraestructura crítica, estableciendo alarmas o avisos en los casos en los que se requiera.
    - Procedimientos de seguridad
    - Procedimientos para la gestión de usuarios y sus accesos al sistema
    - Procedimientos para la gestión de incidentes, gestión de crisis, etc.
    - Procedimientos para la comunicación con los organismos competentes como el CNPIC en cuanto a incidentes, situaciones de riesgos, amenazas y modificaciones de la infraestructura crítica, y también con el CERTSI, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), en cuanto a los posibles ciber-ataques que puedan sufrir, ciber-amenazas que puedan comprometer los sistemas y las redes que soportan la infraestructura crítica.
- De Protección: en este sentido, el CNPIC exige que cada OC incluya en su PPE de cada infraestructura crítica todas las medidas de prevención y detección (*elementos de ciber-seguridad, como firewalls, IPS, IDS, segmentación adecuada de redes, DMZ, etc.*). Y, también, exige que se encuentren definidas las medidas de coordinación y monitorización (como un Centro de Control y Vigilancia, sistemas de alarma y monitorización, sistemas de gestión de crisis, etc.).

8 Recomendaciones elaboración PSO y PPE

8.1 Introducción

Teniendo en cuenta lo revisado anteriormente sobre las políticas y procedimientos definidos por los organismos, se ha podido concluir un carácter mínimo en cuanto al contenido de los PSO y PPE, elementos clave del proceso de adecuación al nivel de seguridad mínimo exigido. Por tanto, a continuación, se desarrollan una serie de recomendaciones para la implantación de las medidas de seguridad integral por parte de cada OC en sus infraestructuras críticas, que complementarán con mayor nivel de detalle los procedimientos y política comentados.
Como ayuda para la elaboración de las recomendaciones, se han utilizado las principales normativas o estándares más relevantes en cada uno de los temas tratados:

- La familia de normas ISO27000 porque es un referente en seguridad internacionalmente aceptado
- ENS porque son los requerimientos de seguridad de las administraciones públicas españolas. Además, también, son un referente en seguridad y están alineadas con las ISO.
- NIST porque es la Organización más conocida en la elaboración de guías de seguridad para los Estados Unidos. Además, también, están perfectamente alineadas con las ISO.

Estas recomendaciones están agrupadas principalmente en dos apartados: uno será la metodología del análisis de riesgos dada su especial relevancia y aspecto principal en los Planes; y el otro apartado serán las medidas de seguridad integral a implementar para la reducción de los riesgos obtenidos del análisis de riesgos.

8.2 Metodología de Análisis de Riesgos

8.2.1 Objetivo

Todo Operador Crítico debe tener desarrollado un Plan de Seguridad para toda la Compañía. El cual deberá estar soportado por un buen análisis de riesgos. Ya que, conociendo los riesgos que pueden afectar a nuestras infraestructuras críticas y sus valoraciones de impacto, nos ayudará como herramienta en la toma de decisiones en la implantación de medidas de seguridad sobre los activos de nuestras infraestructuras críticas.
En este sentido, vamos a definir dos conceptos relevantes:

- Seguridad: es la capacidad que tienen las infraestructuras críticas para resistir las acciones ilegales o malintencionadas que comprometan el servicio prestado por éstas.
- Riesgo: Es una estimación del grado de exposición a que una de las amenazas identificadas se materialice y cause graves daños en nuestras infraestructuras.

Como resultado de la herramienta de análisis y gestión de riesgos, se tomarán decisiones que pueden abarcar desde asumir el riesgo, mitigarlo mediante controles o medidas ya

implantados, invertir en controles o medidas a implantar para mitigar riesgos o también externalizar los riesgos.

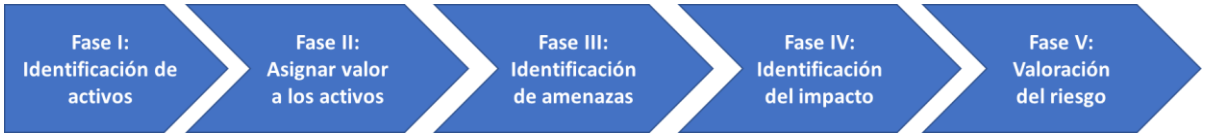
Para la adecuada realización del análisis y gestión de riesgos, será muy importante que participen Responsables de la Compañía de cada uno de los procesos de negocio, de cara a la elaboración de un Mapa de Activos acorde a la situación actual de la Compañía. Así como también, establecer inicialmente un criterio unificado de valoración de estos riesgos y el impacto que estos tienen sobre los activos.

Finalmente, los objetivos principales del proceso de gestión de análisis de riesgos serán los siguientes:

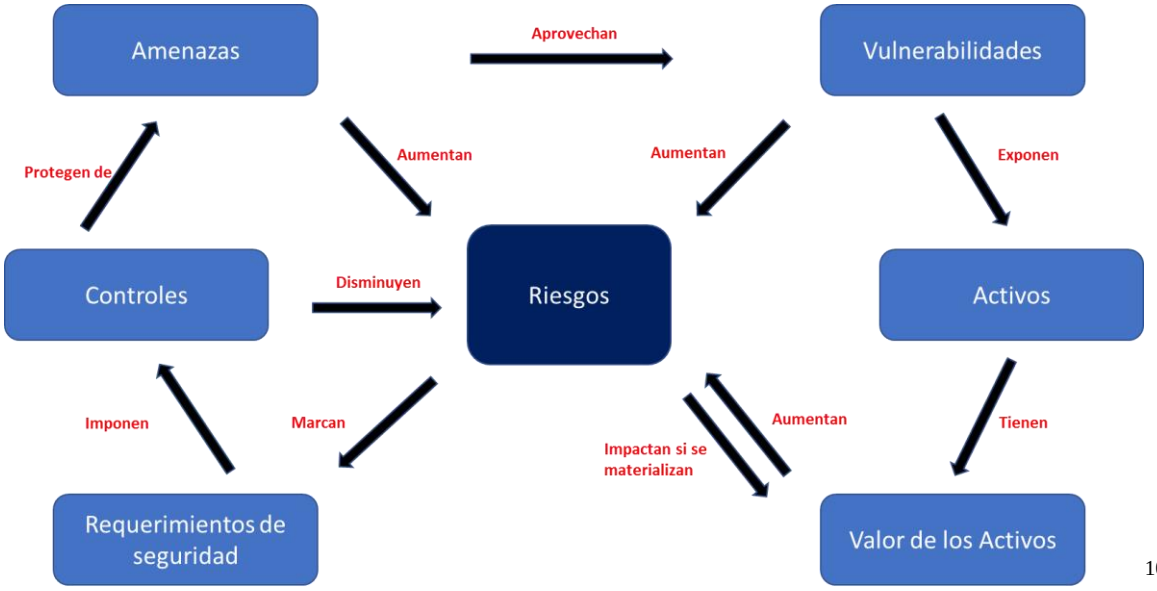
- Identificar la infraestructura tecnológica que da soporte a los procesos de negocio.
    - Entendiendo como activo tecnológico: todo aquel elemento que componen la infraestructura tecnológica que da soporte a los procesos de negocio y que, por tanto, tienen valor suficiente como para justificar su protección.
- Definir la situación actual de los Servicios de Tecnología en cuanto a su disponibilidad y continuidad.
- Valorar el impacto en el negocio, desde la perspectiva de la ausencia de disponibilidad de los sistemas de información, obteniendo:
    - RTO: Tiempo máximo de indisponibilidad.
    - RPO: Cantidad máxima de información que es tolerable perder en caso de incidente grave.
- Identificar los riesgos sobre los activos de información y los activos tecnológicos.
- Identificar los controles propuestos para mitigar el riesgo resultante del análisis, así como los controles ya existentes y su nivel de implantación.
- Analizar los riesgos de incumplimiento y las faltas de alineamiento entre los objetivos y los requerimientos de negocio.
- Presentar escenarios de contingencia sobre los sistemas de información que ocasionen una ausencia de disponibilidad en los procesos de negocio, más de lo que estos pueden asumir.
- Proponer estrategias de recuperación que permitan cumplir con los requerimientos de disponibilidad definidos por negocio.

8.2.2 Descripción

La metodología de análisis de riesgos propuesta se divide en las siguientes fases:



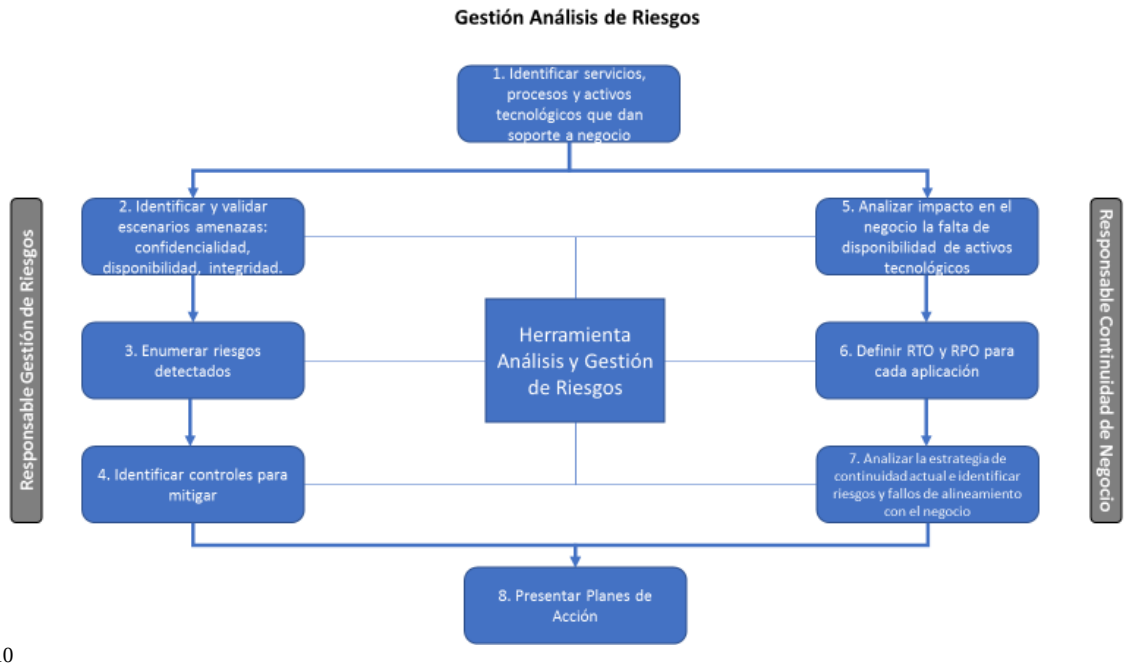
A continuación, se muestra un diagrama de los elementos que intervienen en un análisis de riesgos y cómo estos interactúan entre sí.



[10]

Teniendo en cuenta las fases y los elementos que intervienen en la Metodología de Gestión de Análisis de Riesgos mencionados anteriormente, detallamos a continuación un diagrama del proceso y las tareas a realizar:

[10] AEI Ciberseguridad – Agrupación Empresarial Innovadora



10

8.2.3 Identificación y clasificación de activos

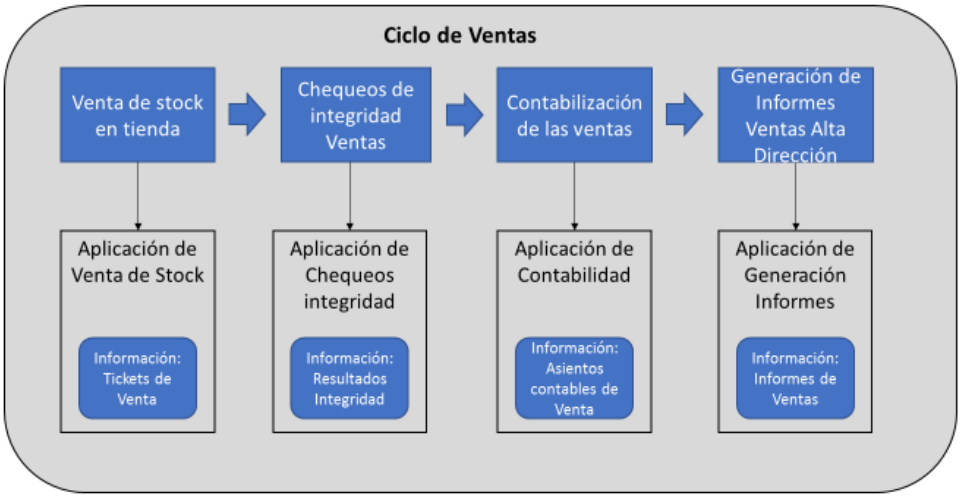
El proceso de identificación y clasificación de activos es el principal y primer punto a tomar en consideración para el análisis y gestión de riesgos. Debido a que, si éste está bien realizado, la toma de decisiones posterior en cuanto a la gestión de los riesgos resultantes será adecuada y completa. Es muy importante ser claros y sinceros, así como detallistas, a la hora de completar este proceso ya que es muy necesario saber de lo que disponemos exactamente, para saber a qué riesgos estamos expuestos. Además, teniendo en cuenta los procesos de negocio críticos para el adecuado funcionamiento de la Compañía, será muy relevante la identificación de la infraestructura de tecnología y comunicaciones que da soporte a los procesos de negocio.
Como resultado de este proceso, obtendremos un Inventario de Activos de la Compañía que estarán clasificados en las siguientes tipologías:

- Procesos de Negocio: Principales ciclos de negocio de la Compañía, a los que un impacto a nivel de confidencialidad, integridad o disponibilidad, tendría graves consecuencias para el adecuado funcionamiento de la Compañía.
- Información Crítica de los Procesos de Negocio: Toda información generada o utilizada en los procesos de negocio de la Compañía, la cual, si se viese afectada en términos de confidencialidad, integridad o disponibilidad, tendría graves consecuencias para el adecuado funcionamiento de la Compañía.
- Aplicaciones relevantes: Todos los procesos de negocio y la información crítica ya comentada se encuentran soportados generalmente sobre aplicaciones informáticas. Y éstas, por tanto, habrá que tenerlas muy en cuenta a la hora de elaborar nuestro Inventario de Activos. Además, se incluirá la tecnología subyacente a estas aplicaciones.

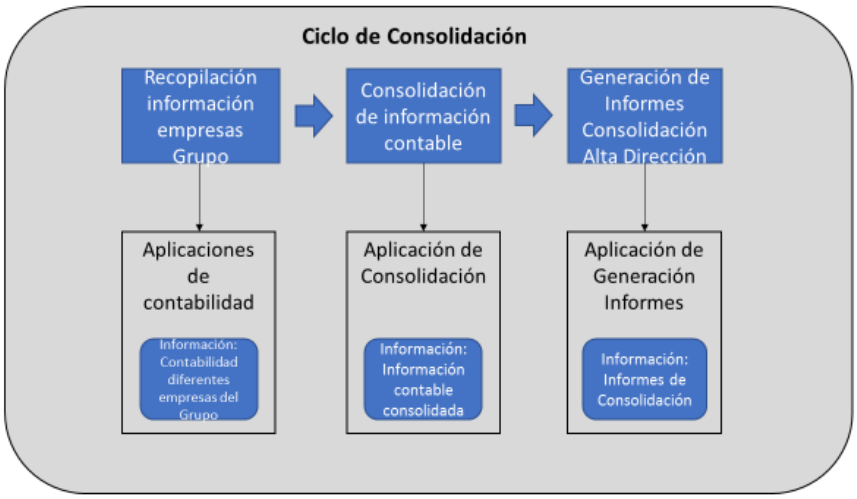
- Servicios de Tecnología: Generalmente, toda empresa que dispone de aplicaciones para soportar sus procesos de negocio gestiona directamente o indirectamente el adecuado funcionamiento de éstas a través de un Departamento de Tecnología o similar, con los servicios que éste pueda ofrecer (*en algunos casos, este servicio se encontrará externalizado en un tercero, el cual también deberá ser incluido en el Inventario de Activos*).
- CPD, Centro de Procesamiento de Datos: Todo el hardware que utilizan las empresas para el mantenimiento de sus aplicaciones, redes de comunicaciones y demás servicios de tecnología, se encuentra generalmente aglutinado en recintos cerrados adecuados para este fin, los CPDs. Dada la criticidad de estos equipos y su ubicación física, deberán ser también incluidos en el Inventario de Activos.
- Servidores: Estos equipos hardware son el principal soporte de las tecnologías utilizadas por la Compañía. Por tanto, todo el detalle de estos (*Modelo, capacidad, tecnología, manuales de usuario, etc.*) deberá ser incluido en el Inventario de Activos.
- Dependencias entre aplicaciones o activos: En multitud de ocasiones, los procesos y subprocesos de negocio se encuentran enlazados o se suceden en cadena y dependen unos de otros para finalizar el proceso a un nivel superior. Y, por tanto, lo mismo ocurre con las aplicaciones a un menor nivel. Es decir, que, si para poder contabilizar mis ventas, primero tendré que registrar y volcar adecuadamente éstas a contabilidad desde los puntos de venta. Y, si en estos procesos, dependientes unos de otros, intervienen varias aplicaciones, existirán también dependencias entre ellas. Por otra parte, también, pueden existir dependencias entre otro tipo de activos, por ejemplo, en comunicaciones. Si tengo flujos de salida de internet, dependeré de líneas de fibra, de firewalls bien configurados, etc.
- Infraestructura de red/comunicaciones: Actualmente, la mayoría de empresas dependen del uso de Internet para el funcionamiento de sus negocios, desde la venta de productos, hasta el uso del correo para las comunicaciones entre los empleados. En este sentido, esta infraestructura adquiere una especial relevancia debido a su utilidad y dependencia existente para el adecuado funcionamiento de los procesos de negocio de la Compañía. Por tanto, será muy importante incluir con gran nivel de detalle todos los componentes que soportan nuestra infraestructura de comunicaciones, tanto interna como externa, así como sus configuraciones de seguridad.
- Ubicaciones físicas donde se encuentran las personas que explotan u operan la información a partir de las aplicaciones: Será muy importante incluir en el Inventario de Activos las ubicaciones físicas donde disponemos al personal necesario para el funcionamiento adecuado de los procesos de negocio de la Compañía.

Para llevar todo este proceso de identificación de activos, se deberán mantener reuniones con los principales Responsables de cada una de las tipologías de activos identificadas anteriormente.

La parte inicial para completar este Inventario de Activos será detallar el más alto nivel: los Procesos de Negocio. Para ello, se deben describir las fases que completan cada proceso de negocio en su orden natural de ejecución, mencionando en cada caso los subprocesos de negocio que también sean necesarios. A continuación, a modo de ejemplo, se detallan dos procesos de negocio: Ventas y Consolidación.



En este diagrama de un ejemplo de un Ciclo de Ventas, se pueden identificar claramente los diferentes subprocesos de negocio de la compañía (*Venta de stock en tienda; Chequeos de integridad de ventas; Contabilización de las ventas; Generación de Informes de Ventas para la Alta Dirección*). También, en estos subprocesos se genera la información crítica de cada uno de ellos (*Tickets de Venta; Resultados de los chequeos de integridad; Asientos contables de ventas; Informes de Ventas*), así como las aplicaciones de la Compañía que soportan estos procesos y almacenan la información crítica comentada (*Aplicación de Venta de stock; Aplicación que realiza los chequeos de integridad; Aplicación que contabiliza los asientos de venta; Aplicación que genera los Informes de Venta*).



En este diagrama de un ejemplo de un Ciclo de Consolidación, se pueden identificar claramente los diferentes subprocesos (*Recopilación de información de las empresas del Grupo; Consolidación de información contable; Generación de Información de*

Consolidación para la Alta Dirección). También, en estos subprocesos, se genera la información crítica de cada uno de ellos (*Información de contabilidad de las diferentes empresas del Grupo; Información contable consolidada; Informes consolidados*), así como las aplicaciones de la Compañía que soportan estos subprocesos y almacenan la información crítica comentada (*Aplicaciones de contabilidad; Aplicación que realiza el proceso de consolidar la información contable; Aplicación que genera los Informes consolidados*).

Muy importante, será también identificar correctamente aquellos procesos, subprocesos y mantenimiento de aplicaciones que se encuentren externalizados en terceros. Esto con el objetivo de definir las dependencias que puedan existir de otras compañías. Como pudiera ser el mantenimiento de alguna aplicación específica, las comunicaciones hacia el exterior, la telefonía, el almacenamiento del hardware, etc.

Siguiendo con el Inventario de Activos, bajaremos de nivel relacional y procederemos a detallar la información crítica y las aplicaciones relacionadas con cada subproceso y proceso de negocio, hasta finalizar con el responsable para cada uno de estos activos.

A modo de recomendación, se proponen los siguientes conceptos agrupados en tipología y nivel de agregación (*el documento se ha ubicado en el Anexo del Proyecto*) como resultado final del Inventario de Activos:

- Nivel: Procesos de negocio
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
- Nivel: Información crítica
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica
    - Propietario de la información
- Nivel: Aplicaciones
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica
    - Propietario de la información
    - Aplicación que soporta
    - Responsable de la aplicación
- Nivel: Servicios de Tecnología
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica

    - Propietario de la información
    - Aplicación que soporta
    - Responsable de la aplicación
    - Servicio Tecnología
    - Responsable Servicio Tecnología
- Nivel: CPD (Centro de Procesamiento de Datos)
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica
    - Propietario de la información
    - Aplicación que soporta
    - Responsable de la aplicación
    - Servicio Tecnología
    - Responsable Servicio Tecnología
    - CPD
- Nivel: Servidores
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica
    - Propietario de la información
    - Aplicación que soporta
    - Responsable de la aplicación
    - Servicio Tecnología
    - Responsable Servicio Tecnología
    - CPD
    - Servidores
    - Responsable Servidores
- Nivel: Dependencias entre activos
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio
    - Responsable
    - Información crítica
    - Propietario de la información
    - Aplicación que soporta
    - Responsable de la aplicación
    - Servicio Tecnología
    - Responsable Servicio Tecnología
    - CPD
    - Servidores
    - Responsable Servidores
    - Dependencias entre activos
- Nivel: Infraestructura de red
    - Compañía
    - Proceso de Negocio
    - Sub-Proceso de Negocio

- Responsable
- Información crítica
- Propietario de la información
- Aplicación que soporta
- Responsable de la aplicación
- Servicio Tecnología
- Responsable Servicio Tecnología
- CPD
- Servidores
- Responsable Servidores
- Dependencias entre activos
- Infraestructura de red

8.2.4 Valoración de los activos

En este apartado, se identificará cuánto valor tienen los activos para la empresa. Es decir, cuál puede ser el impacto de que uno de sus activos resulte dañado.
Para los activos de información, la forma de valorar esto se realiza a través de los conceptos: disponibilidad, integridad y confidencialidad. Aunque también, se podrían incluir otros como tener impacto en la reputación de la Compañía, en el medio ambiente, daño a personas, etc. Y, en cuanto a los activos físicos, además de los últimos mencionados, se podría añadir el coste económico.
Entonces, para aquellos casos en los que no sea posible la valoración cuantitativa, se utilizarán escalas cualitativas como: bajo, medio, alto; o del 1-10.

Para llevar a cabo este complicado proceso de valoración de los activos, se han desarrollado a continuación una serie de cuestionarios para conocer de primera mano el valor que tienen los procesos de negocio y la información crítica generada por estos.

8.2.4.1 Cuestionario Conocimiento del Proceso de Negocio

- En primer lugar, habrá que realizar una descripción del proceso de negocio en cuestión.

A continuación, indicaremos los requisitos de recuperación de la información en caso de incidente grave:

1. ¿Cuánto tiempo puede permitirse la paralización del proceso sin afectar a la continuidad de la Compañía, su imagen pública, problemas legales serios o consecuencias graves contra los empleados?
2. En caso de incidente grave que ocasione pérdida de información de los sistemas informáticos, ¿cuál es el tiempo máximo asumible de pérdida de información?
3. ¿Existen momentos específicos en los que el proceso sea especialmente crítico?

Ahora, en el caso de que se produzca una interrupción prolongada, ¿cuáles serían las consecuencias?

- Consecuencias legales
  - Sin impacto
  - Trivial
  - Relevante
  - Crítico
- Consecuencias financieras
  - <1% cifra de negocio
  - 1%<X<33%
  - 33%<X<66%
  - 66%<X<100%
- Consecuencias laborales
  - Ningún empleado
  - Afecta levemente a algunos
  - Afecta a muchos empleados
  - Afecta a toda la Compañía
- Consecuencias de imagen
  - Sin impacto
  - Repercusión interna
  - Repercusión externa
  - Repercusión en los medios de comunicación
  - Repercusión a la sociedad
- Consecuencias operativas
  - Sin impacto
  - Ineficiencia en procesos
  - Interrupción en servicios internos
  - Interrupción en servicios externos
  - Continuidad de la Compañía
  - Afecta a otras Compañías

Es relevante comentar que este cuestionario deberá ser rellenado para cada uno de los procesos de negocio identificados como críticos.

8.2.4.2 Cuestionario Conocimiento sobre la Información de Negocio

En primer lugar, habrá que realizar una descripción de la información crítica a valorar.

- Y, por otra parte, dónde se encuentra esta información almacenada:
  - Papel
  - Aplicaciones
  - Correos
  - Discos Duros
  - Nube
  - Caja Fuerte
  - Etc.
- ¿Dónde se encuentran las personas responsables del manejo y custodio de la información?
- ¿Se ha procedido a subcontratar la creación o tratamiento de esta información?

- Si la información se pierde o elimina accidentalmente, ¿qué medios informáticos se podrían utilizar para recuperarla?
    - Ordenador
    - Disco duro
    - Backup
    - Cinta
    - Proveedor

A continuación, procederemos a valorar la criticidad de la información aquí analizada:

- Consecuencias de una divulgación no autorizada a personal externo de la Compañía:
    - Consecuencias Legales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias económicas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias laborales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias de imagen
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias operativas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
- Consecuencias de una divulgación no autorizada a personal interno de la Compañía:
    - Consecuencias Legales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias económicas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias laborales

        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias de imagen
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias operativas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
- Consecuencias de una pérdida irreversible de la información:
    - Consecuencias Legales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias económicas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias laborales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias de imagen
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias operativas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
- Consecuencias de la aparición de errores en la información:
    - Consecuencias Legales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias económicas
        - Sin impacto
        - Trivial
        - Relevante

        - Crítico
    - Consecuencias laborales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias de imagen
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias operativas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
- Consecuencias de una manipulación fraudulenta de la información con intención de perjudicar:
    - Consecuencias Legales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias económicas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias laborales
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias de imagen
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico
    - Consecuencias operativas
        - Sin impacto
        - Trivial
        - Relevante
        - Crítico

Es relevante comentar que este cuestionario deberá ser rellenado para cada una de las informaciones críticas identificadas.

8.2.4.3 Valoración de los activos físicos

Para el caso concreto de los activos físicos, se deberá unificar el criterio de valoración, así como también reunir a todos los responsables implicados en la valoración de cada uno de estos activos. Además, en aquellos casos que aplique, se deberán incluir también a los proveedores que nos proporcionan los activos o si los tenemos subcontratados.
A continuación, se presentan algunos ejemplos:

<table>
<tr><th>Valor</th><th>Reducción del beneficio</th><th>Salud y Seguridad</th><th>Entorno natural</th><th>Patrimonio Social/Cultural</th><th>Comunidad/ Gobierno/ Reputación</th><th>Legal</th></tr>
<tr><td>5</td><td>20MM-300MM€</td><td>Múltiples víctimas o efectos irreversibles >100 personas</td><td rowspan="2">Efectos muy graves que a largo plazo afectan al ecosistema</td><td>Daños muy graves en estructuras</td><td>Huelgas severas y duraderas con impacto a nivel internacional</td><td>Persecución y sanciones significativas</td></tr>
<tr><td>4</td><td>1MM-20MM€</td><td>Sólo una víctima mortal o discapacidad irreversible</td><td rowspan="2">Daños permanentes en estructuras</td><td>Protestas a nivel nacional</td><td>Incumplimiento de legislación grave</td></tr>
<tr><td>3</td><td>200.000-1MM€</td><td>Discapacidad <30%</td><td>Efectos serios a medio plazo</td><td>Atención significativa</td><td>Incumplimiento de legislación con investigación</td></tr>
<tr><td>2</td><td>50.000-200.000€</td><td>Hospitalización</td><td>Efectos a corto plazo que no afectan al ecosistema a largo plazo</td><td>Daños graves pero reparables</td><td>Atención en medios y comunidades locales</td><td rowspan="2">Aspectos legales menores</td></tr>
<tr><td>1</td><td><50.000€</td><td>No implica tratamientos médicos</td><td>Efecto menor sobre el medio</td><td>Impactos menores</td><td>Quejas sociales</td></tr>
</table>

Ahora, una vez obtenidas las valoraciones de los activos (procesos de negocio, información y activos físicos), la cuestión se centra en identificar cuáles de ellos serán críticos. Y también definir la prioridad de estos a restaurar en caso de que tenga lugar una situación de contingencia.

Para la definición de la criticidad, existen multitud de formas de hacerlo en base a los datos obtenidos anteriormente, a partir de los cuestionarios y la tabla de valoración de activos

físicos. Pero aquí propondremos una forma sencilla y eficaz: para las valoraciones cualitativas de procesos de negocio e información, se considerarán como críticas aquellos que hayan sido considerados como relevantes o críticos en cualquiera de los conceptos indicados. Y, en el caso de los activos físicos, dado que se valoran tres conceptos (confidencialidad, disponibilidad e integridad), se realizará un cálculo sencillo como la suma del valor asignado a cada uno de ellos (1-5) y, en el caso de que la suma de estos tres supere el 5, será considerado como crítico.

Otra forma más gráfica sería la siguiente (intervalos ejemplo asociados a la criticidad valorada por el personal de negocio):

RTO (Tiempo máximo de indisponibilidad)	**Descripción**
5min – 12h	Crítico
12h – 1 día	Elevado
1día – 3días	Moderado
3días – 1semana	Bajo
> 1semana	Muy bajo
RPO (Cantidad máxima de información tolerable a perder)	**Descripción**
5min – 12h	Crítico
12h – 1 día	Elevado
1día – 3días	Moderado
3días – 1semana	Bajo
> 1semana	Muy bajo

Como resultado del análisis de impacto en el negocio, se obtiene una valoración de las necesidades de disponibilidad de los sistemas y recursos asociados a los procesos.
De esta forma, ya tendremos valorados los activos de nuestra organización e identificados mediante un criterio adecuado y sencillo cuáles de ellos habrá que considerar como críticos.

8.2.5 Identificación de las amenazas

Una vez identificados y valorados todos los activos, el siguiente paso será identificar las amenazas que pueden ocasionar graves daños sobre estos activos para la Compañía.

Una amenaza se define como un evento que se puede convertir en un incidente, si ocasiona daños materiales o inmateriales para la Compañía.

Es muy importante hacer una adecuada y completa identificación de las amenazas teniendo en cuenta los activos de la Compañía. Para que, de esta manera, la Compañía pueda anticiparse a la materialización de estas amenazas, impidiendo la aparición de daños o reduciendo su impacto.
Las amenazas podrían ser tanto físicas como lógicas, pero dado el carácter de este proyecto en cuanto a la ciberseguridad, nos centraremos en las lógicas. En este sentido, algunos ejemplos: ataque de ransomware, abuso de privilegios de acceso, ataques de denegación de servicio, manipulación de las configuraciones, difusión de malware, etc.

Dentro de las amenazas, hay que distinguir aquellas intencionadas de las no intencionadas, y aquellas ejecutadas por personal interno o externo a la Compañía.

Todas estas amenazas no afectan por igual a todos los activos, sino que dependerá del tipo de Organización, de su estructura, de los activos críticos que disponga y de las medidas de seguridad que tenga implantadas. Las amenazas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda ser explotada por la amenaza para transformarse en un incidente con impacto en la Compañía.
En base a esto, decir que una vulnerabilidad no es algo grave hasta que ésta no es explotada. Es entonces cuando sí requiere de especial atención para la Compañía. Sin embargo, a las Compañías se recomienda que lleven a cabo una defensa proactiva de sus activos más críticos, adelantándose al incidente. Y no reactiva, es decir, esperando a que el incidente tenga lugar, para ejecutar planes específicos para su resolución.

A partir de esto, surgen los llamados escenarios de contingencia, es decir, aquellas situaciones en las que una vulnerabilidad puede ser explotada y esta situación se puede dar en nuestra Organización.

Las típicas amenazas que suelen considerarse son:

- Fuego en el Centro de Procesamiento de Datos
- Accidente industrial
- Terremoto en las instalaciones principales de la Compañía
- Inundaciones en las instalaciones principales de la Compañía
- Corte de las comunicaciones principales
- Caída del alumbrado eléctrico
- Boicot terrorista
- Descarga eléctrica extrema por aparato eléctrico
- Etc.

Pero, atendiendo en lo relativo a la ciberseguridad, consideramos las siguientes amenazas:

- Ataque de denegación de servicio
- Caída de los servidores
- Corte de las comunicaciones
- Manipulaciones de la maquinaria industrial
- Acceso y robo de información confidencial
- Suplantación de identidad
- Etc.

Entonces, para cada una de las amenazas identificadas, habrá que analizar su probabilidad de ocurrencia y la probabilidad de que, si ésta se materializa, tengan lugar daños en la Organización.

8.2.6 Identificación de impactos

Cuando una vulnerabilidad es aprovechada y se materializa, convirtiéndose en un incidente, como consecuencia surge el impacto del ataque en los activos de la Compañía.
En este sentido, se trata de medir el impacto del incidente sobre nuestros activos, sabiendo la valoración de estos y los daños que estos pueden sufrir.

Entonces, teniendo en cuenta la identificación de activos críticos realizada, el impacto en el negocio a través de la valoración de los activos, obteniendo una ausencia de disponibilidad de los activos en caso de incidente, disponemos del RTO máximo (tiempo máximo de indisponibilidad) y el RPO máximo (la cantidad máxima de información que es tolerable perder en caso de incidente grave); y, por último, habiendo analizado los riesgos de incumplimiento y faltas de alineamiento entre los objetivos y los requerimientos de negocio, se pueden presentar los impactos de las amenazas sobre los activos de la Compañía.

Para lo cual, se propone llevar a cabo tablas como la siguiente:

Ciber - Amenaza	Impacto	Alcance servicios afectados
Ataque denegación de servicio	Paralización temporal de los sistemas de información que no estén dispuestos en modo de alta disponibilidad. Aquellos que se encuentren implementados de esta manera, podrá funcionar de manera automática. En el caso de que no existiera o no se activase el CPD de respaldo, podría tener graves consecuencias para la Compañía, así como	Activos y servicios prestados que se queden caídos y no se restablezcan instantáneamente.

	para la recuperación de la información. Que, en este caso, dependería del backup.	
Malware/Ransomware	Dependiendo de las personas afectadas y la información afectada, las repercusiones pueden ser muy graves para la Organización ya que puede tratarse de información sumamente confidencial o crítica para su operativa diaria.	Información de clientes. Información de la Compañía.

A continuación, se presenta un ejemplo de valoraciones de activos en cuanto al valor que tienen para el negocio y su estrategia de recuperación:

Aplicación/ Servicio	**Arquitectura**	**Estrategia recuperación actual**	**RTO actual**	**RTO objetivo**	**RPO actual**	**RPO objetivo**
App1	Tipología (desarrollo propio, adquisición comercial, etc.)	Aprovisionamiento hardware + Instalación Sistema Operativo y Parches + Instalación SGBD + Conexión con SAN (red de área de almacenamiento) y NAS (almacenamiento en red) de respaldo.	1 semana	5 días (*Este dato dependerá de las necesidades de negocio*)	Sistema Operativo: N/A; Aplicación: 1día; Datos: 5min;	Sistema Operativo: N/A; Aplicación: 1día; Datos: 5min; (*Este dato dependerá de las necesidades de negocio*)
App2	Alta disponibilidad servidores	Arranque desde nodo clúster en CPD secundario (automático o manual)	12h	10h (*Este dato dependerá de las necesidades de negocio*)	Sistema Operativo: No; Aplicación: N/A; Datos: 5min;	1 día (*Este dato dependerá de las necesidades de negocio*)

8.2.7 Valoración del riesgo

El riesgo queda definido como la medida del daño probable sobre un sistema. Al final, hablar de riesgo, es hablar de la probabilidad de que un incidente tenga un impacto sobre los activos de la Compañía.
En este sentido, como metodología de valoración del riesgo, se define lo siguiente:

Si tenemos una amenaza sobre nuestros sistemas, la probabilidad de que ocurra y se materialice, lo llamaremos Potencial de la Amenaza, que será la primera parte de la Valoración del Riesgo. Después, habiendo identificado y valorado correctamente nuestro inventario de activos, podremos evaluar y valorar el impacto de esa potencial amenaza sobre nuestros activos, que consecuencias tendría. Cabe destacar que los activos de nuestro inventario llevan asociados un riesgo propio del activo, el cual llamaremos riesgo inherente. Y, por último, si tenemos en cuenta el riesgo inherente propio del activo, el potencial de la amenaza y la valoración del activo con los sistemas de seguridad implantados que le afecten, nos quedará como resultado un riesgo residual.

Las fases para el cálculo del riesgo quedarían de la siguiente manera:

Ahora, se procede a cuantificar el riesgo existente sobre los activos identificados (procesos de negocio, activos de información y activos tecnológicos) teniendo en cuenta todas las salvaguardas y medidas aplicadas (controles implementados, firewalls, IPS, IDS, segmentación de red, servicios en alta disponibilidad, RTO y RPO, posibilidades de recuperación, etc.).

En el siguiente cuadro, se describe un ejemplo de la valoración del riesgo. Para la cual, habrá que tener en cuenta lo siguiente:

- El potencial de la amenaza es un compromiso entre el grado de vulnerabilidad del activo y la frecuencia de la amenaza.
  - 1 – Muy bajo
  - 2 – Bajo
  - 3 – Medio
  - 4 – Alto
  - 5 – Muy alto
- La valoración del impacto será el dato proporcionado por el personal de negocio con respecto a cómo afectaría cada amenaza en un activo durante un periodo determinado.
- El riesgo inherente queda calculado como: Potencial de la amenaza x Valoración del Impacto.

- El riesgo residual ha sido calculado en base al riesgo inherente y al grado de madurez que tengan las contramedidas implantadas y valoradas por el personal de IT.

En este caso, se está asumiendo un nivel de riesgo aceptable por encima de 6.

Amenaza	Activo	Incidencia	Potencial de la amenaza	Valoración del impacto	Riesgo inherente	Riesgo residual
Ataque Denegación de Servicio	App1	Indisponibilidad > 1h	3	4	12	10,13
Malware/ Ransomware	Info1	Fuga información	3	3	9	7,6
Manipulación industrial	App1	Error/Manipulación	3	4	12	11
Ciberataque	BBDD1	Pérdida de información	2	3	6	6

Después de este cálculo, la Compañía ya tendría la suficiente información como para llevar a cabo algunas decisiones con respecto a las amenazas, los activos y los riesgos que superan el umbral definido como aceptable:

- Eliminar el activo, valorando si se puede prescindir de él.
- Implantar nuevas salvaguardas/medidas de seguridad o mejorar las ya existentes para reducir el riesgo hasta niveles aceptables.
- Transferir el riesgo a terceras partes.

8.2.8 Herramientas gestión de análisis de riesgos

Para facilitar este proceso de gestión de análisis de riesgos, es muy recomendable hacer uso de algunas herramientas disponibles en el mercado. Aunque también habrá que tener muy en cuenta consideraciones muy importantes antes de realizar esta adquisición:

- Hay que tener en cuenta que estas herramientas suelen estar ya prediseñadas para una metodología específica de análisis de riesgos.
    - Lo que implica que podrá tener ya definidas las amenazas, los riesgos, etc.
- También habrá que valorar las posibilidades que ofrece de mantenimiento
- Por otra parte, será importante para nosotros si pretendemos que esta herramienta esté interconectada con otros sistemas de la Compañía.

Aunque, también existe la posibilidad de desarrollar una herramienta propia de gestión de análisis de riesgos.

8.3 Medidas de seguridad

8.3.1 Gestión de la seguridad

Una vez la Compañía ha decidido el umbral de aceptación del riesgo, ejecutado el análisis de riesgos y obtenido los resultados, la Compañía tendrá que tomar decisiones con todos los resultados obtenidos. Para lo cual, se elabora un Plan de Seguridad, cuyo objetivo es implantar las contramedidas, procesos y procedimientos de seguridad para asegurar siempre que el nivel de exposición al riesgo de la Compañía siempre está por debajo del umbral de riesgo definido en el análisis de riesgos.

Y, dado que este umbral se caracteriza por el cumplimiento de los tres conceptos básicos relativos a los activos críticos identificados, este Plan estará principalmente desarrollado para asegurar el cumplimiento de los niveles mínimos de confidencialidad (*la información sólo es accesible por las personas autorizadas y así definidas*), integridad (*la información se asegura completa y exacta*) y disponibilidad (*el acceso a la información se mantiene siempre que se haya definido por los requisitos de negocio*) para cada uno de los activos críticos definidos en la Gestión del Análisis de Riesgos.

Dado el carácter dinámico de las Organizaciones, así como también de las amenazas que cada día aumentan, varían y se vuelven cada vez más complejas, será muy importante que el Plan de Seguridad de la Compañía también sea un Plan dinámico y la herramienta en la que se encuentre desarrollado sea también de fácil actualización y/o modificación. Atendiendo además a las innovaciones tecnológicas, las nuevas regulaciones y normativas a las que la Compañía se vea expuesta y cualquier otro evento o circunstancia que le pueda afectar, que también deberá ser tenido en cuenta y, por tanto, añadido al Plan de Seguridad. Además, para cumplir esto, será muy importante que, en el desarrollo y mantenimiento del Plan, participen especialistas de las diferentes áreas, terceros y administraciones públicas que así lo requieran.

Para que este Plan sea efectivo, deberá ser promovido y defendido por la Dirección y Alta Dirección de la Compañía involucrándose y haciéndose partícipe en todo momento.
Por otra parte, para el adecuado diseño y mantenimiento del Plan, deberán participar personas multidisciplinares de diferentes áreas de la Compañía. Y, para su adecuada gestión, se recomienda crear un Comité de Gestión encargado del diseño, desarrollo y cumplimiento en base a los criterios que se hayan definido previamente.
Este Comité deberá ser totalmente independiente y autónomo en la toma de decisiones con respecto a la elaboración del Plan.

También, y de cara a hacer visible el apoyo por parte de la Dirección al desarrollo y ejecución del Plan de Seguridad, se deberán llevar a cabo ciertas actuaciones como:

- Comunicaciones a la Compañía de la importancia de la elaboración del Plan y la participación de todos los empleados. Mediante campañas de formación, sensibilización, etc.
- Asegurando que los objetivos del Plan de Seguridad quedan adecuadamente definidos, así como claros y sencillos de su cumplimiento.

- Llevando a cabo revisiones periódicas del Plan de Seguridad.
- Asegurando la disponibilidad de los recursos necesarios para la viabilidad del Plan de Seguridad.

El Comité de Gestión deberá estar formado por:

- El Responsable del Comité: Sus funciones son a alto nivel en cuestiones de estrategia. Deberá desarrollar la Política del Plan de Seguridad, estableciendo sus objetivos y los roles, y asegurando su cumplimiento, comunicará a la Compañía la necesidad de su cumplimiento y de su mejora continua. Además, deberá de proporcionar los recursos necesarios para crear, implementar, operar, supervisar, mantener y mejorar el Plan de Seguridad. Y, también, velar por la realización de las revisiones periódicas, asegurando además la integridad y resolución de las auditorías del Plan llevadas a cabo, verificando el cumplimiento de los controles o las recomendaciones de las auditorías.
- Responsable del SGSI (*Sistema de Gestión de Seguridad de la Información*): Es el encargado de cumplir con las directrices de la Dirección de la Compañía. Propondrá los roles, recursos necesarios, estrategias, etc. encaminados a conseguir los objetivos de seguridad. También, se encargará de las revisiones y mejoras del Plan, actualización de procedimientos, etc.
- Responsable de Seguridad: Sus funciones son la realización del análisis de riesgos, la definición del umbral de riesgo aceptable, evaluación e implantación de contramedidas, definición del Responsable del Comité, etc.
- Responsable de área o Departamento: Deberá de trasladar las necesidades de negocio de su área para el adecuado análisis de riesgos.

Y, con el objetivo de obtener experiencias de otras Compañías, así como un adecuado asesoramiento por parte de organismos especializados, se recomienda mantener un contacto constante con los siguientes organismos:

- CNPIC: Centro Nacional para la Protección de las Infraestructuras Críticas
    - Es el órgano director y coordinador de cuantas actividades relacionadas con la protección de las infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior, a la que está adscrito.
    - Su principal objetivo es prestar una eficaz colaboración para mantener seguras las infraestructuras críticas españolas que proporcionan los servicios esenciales a nuestra sociedad.
- ICS – CERT: Industrial Control Systems Cyber Emergency Response Team
    - Ofrece un sistema de control de seguridad en colaboración con la US-CERT enfocado para:
        - Responder y analizar sistemas de control relacionados con incidentes.
        - Vulnerabilidad y análisis del malware.
        - Proveer soporte in situ para respuesta a incidentes y análisis forense.
        - Proporcionar conocimiento de la situación en forma de inteligencia procesable.

        - Coordinar la divulgación responsable de vulnerabilidades / mitigaciones.
        - Compartir y coordinar la información sobre la vulnerabilidad y el análisis de amenazas a través de productos de información y alertas.

    El ICS-CERT es un componente clave de la Estrategia de Seguridad de los Sistemas de Control.

- CCN – CERT, CNI: Centro Nacional de Inteligencia
    - Es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del CNI (Centro Nacional de Inteligencia).
    - Su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). Para lograr su objetivo, responden de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontan de forma activa las nuevas amenazas existentes.
- INTECO (*Instituto Nacional de Tecnologías de la Comunicación*) – INTECO Cert (*Centro de Respuesta a Incidentes de Seguridad*)
    - INTECO tiene encomendadas las misiones de sentar las bases de coordinación de distintas iniciativas públicas en torno a la seguridad informática, impulsar la investigación aplicada y la formación especializada en el ámbito de la seguridad en el uso de las TIC y convertirse en el Centro de Referencia en Seguridad Informática a nivel nacional.
- Guardia Civil – GDT (*Grupo de Delitos Telemáticos*)
    - El GDT está creado para perseguir los delitos informáticos. Si se identifica en la entidad un problema de seguridad en la red, un contenido ilícito o detectamos u observamos una conducta que pudiera ser delictiva, se deberá comunicarlo al GDT. Todo lo que en ella se recibe es tratado con la máxima discreción.
- Cuerpo Nacional de Policia
    - El desarrollo de la Sociedad de la Información y la difusión de los efectos positivos que de ella se derivan exigen la generalización de la confianza de los ciudadanos en las comunicaciones telemáticas. Como respuesta a esta necesidad, y en el marco de las directivas de la Unión Europea, el Estado español ha aprobado un conjunto de medidas legislativas, como la Ley de Firma Electrónica y el RD sobre el Documento Nacional de Identidad electrónico, para la creación de instrumentos capaces de acreditar la identidad de los intervinientes en las comunicaciones electrónicas y asegurar la procedencia y la integridad de los mensajes intercambiados.
- AEI Seguridad
    - La Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del sector de las Nuevas Tecnologías, sus industrias afines y auxiliares, así como otros sectores emparejados con el mismo, que deseen contribuir a los fines de la Asociación, en el ámbito nacional de las Tecnologías de Seguridad.
- McAfee Alerta
    - Avisa a los usuarios de las nuevas y peligrosas amenazas que se pueden encontrar en la red. Se trata de evitar ser víctimas de los peligros online. Nos ofrecerá: actualizaciones de firmas malware, alertas de nuevas amenazas, notificaciones de .DAT, notificaciones de seguridad, etc.

- Symantec
    - Symantec ayuda a los consumidores y a las organizaciones a proteger y administrar su información. Sus servicios y programas protegen contra una mayor cantidad de riesgos en más puntos y de una forma más completa y eficaz, lo que brinda tranquilidad sin importar dónde se utilice o almacene la información.

Por otra parte, con respecto a la necesidad de permitir el acceso a la información de la Compañía por parte de terceros, se implantarán los controles necesarios para su control y supervisión. Asegurando que únicamente los terceros y las personas autorizadas acceden a la información. Además, se monitorizarán en todo momento sus actividades, dejando siempre registro de éstas para que, en caso de sospechar o producirse actividades no autorizadas, siempre se puedan tener evidencias de estas actividades no autorizadas para, en su caso, proceder a las acciones correspondientes.

También, de cara a ayudar con algunos aspectos en la elaboración del Plan de Seguridad, mantenimiento y mejora de éste, se recomienda utilizar algunas herramientas como, por ejemplo:

- Gestor documental
- Gestor de flujos de trabajo
- Cuadros de Mando
- Cortafuegos
- Control de Acceso a Listas
- Etc.

En cuanto a los aspectos formativos, cabe destacar la relevancia que adquieren los conceptos formación y concienciación para el éxito del Plan de Seguridad. Es de vital importancia que exista una formación a todos los niveles de la Compañía, con el principal objetivo de que los empleados estén concienciados del Plan y de las ventajas que aporta a la Compañía y a los mismos empleados. Ya que, de esta manera, se adopta una forma proactiva de seguridad que se inicia en los propios empleados, como la primera barrera de defensa ante ciber-amenazas.

Esto se puede llevar a cabo mediante cursos formativos, paneles descriptivos en las instalaciones de la Compañía, carteles, charlas, debates, foros, etc.
Esto implica que todos los empleados de la Compañía, así como usuarios externos y terceros, cuando desempeñen actividades de la propia Compañía, deberán recibir esta formación. Y, también, será muy importante que esta formación sea actualizada adecuadamente de forma periódica de cara a estar completamente alineada con las políticas, normas y procedimientos que apliquen dentro del Plan de Seguridad.

8.4 Medidas técnicas

8.4.1 Seguridad en la red

Dependiendo del funcionamiento de cada Compañía y de los servicios prestados, podrá adquirir mayor o menor relevancia este apartado, ya que dependerá mucho de si la Compañía utiliza Internet para sus servicios.
Pero, en la mayoría de los casos, las Compañías harán uso de Internet y, además, internamente, dispondrán de su propia red de la Compañía.
El punto más crítico de este apartado es que esta red interna de la Compañía se encuentre perfectamente segmentada, es decir, que los equipos informáticos donde resida la información más sensible o los servicios más críticos, se encuentren perfectamente aislados del resto de la red de la Compañía. De esta forma, se consigue que, en el caso de que la red sea atacada y consigan acceder a la red interna de la Compañía, no tengan visibilidad y, por tanto, tampoco acceso a esta parte crítica de la Compañía.

Inicialmente, existen varias opciones a la hora de analizar la seguridad en la red de nuestra Compañía:

- Conexiones a redes de otras Compañías
- Redes Privadas Virtuales / Accesos remotos
- Conexiones inalámbricas no seguras
- Puertos no protegidos adecuadamente
- Puertas traseras
- Etc.

En este sentido, mencionamos a continuación algunos puntos críticos a tener en cuenta:

8.4.2 Cortafuegos

Se deberá crear una adecuada política de cortafuegos: Es decir, a partir de una adecuada configuración de seguridad, se podrá controlar todo el tráfico de red entrante y saliente. El cual podrá ser filtrado por direcciones IP, protocolos o aplicaciones específicas. En principio, a través del adecuado análisis de riesgos, se podrá saber exactamente qué tipo de tráfico de red entrante y saliente es necesario para el adecuado funcionamiento de la Compañía. En este sentido, todo aquel que difiera de este tráfico, deberá ser bloqueado.
Además, los principales tipos de configuraciones de cortafuegos son: filtrado de paquetes; inspección de estados; Proxy.
Por otra parte, a través de estos cortafuegos, se pueden implementar las segmentaciones de red, creando así las zonas desmilitarizadas (*DMZ*), donde se aislarán los activos o servicios más críticos.

8.4.3 Auditoría

Una vez el Plan de Seguridad se haya diseñado, implantado y esté operando adecuadamente, con sus correspondientes revisiones periódicas y mejoras, será muy recomendable realizar periódicamente procesos de auditoría tanto interna como externa. De esta manera, la Compañía se asegura el correcto funcionamiento del Plan.
La importancia de realizar auditorías, además de las revisiones periódicas ya comentadas, radica en la participación de personal ajeno a estas actividades. Como bien puede ser el Dpto. Auditoría Interna, para el caso de ejecutar auditorías internas; y un tercero, para el caso de ejecutar auditorías externas.
En el caso de llevar a cabo auditorías internas, la Compañía deberá asegurarse que este Dpto. dispone del persona apropiado y adecuadamente formado en esta materia. Y, por tratarse de un Dpto. independiente de todo el personal que participa en la elaboración del Plan de Seguridad, nos aseguramos que las conclusiones del proceso de auditoría serán totalmente objetivas.
Y, para un mayor grado de éxito, se podrán llevar a cabo auditorías externas por terceros especializados en esta materia.

A partir de estas auditorías, surgirán recomendaciones y aspectos identificados que deberán ser evaluados y, en su caso, resueltos por la Compañía en el Plan de Seguridad.

8.4.4 Aseguramiento de equipos

Como parte de la ciber-seguridad de la Compañía, es muy importante la adecuada configuración de los dispositivos electrónicos, ya sea desde un servidor, un antivirus, etc. Para lo cual, se debe realizar un adecuado bastionado estableciendo procedimientos de bastionado por tipología de dispositivo en la Compañía.

En primer lugar, se deberá llevar a cabo la creación de políticas y controles para el bastionado para implementar en los dispositivos bajo alcance. Por ejemplo, pueden ser el adecuado parcheo, actualización de equipos, realización de copias de seguridad, control de accesos, etc.

A continuación, se detallan algunos aspectos a tener en cuenta.

8.4.4.1 Gestión de Permisos

En este sentido, se recomienda en primer lugar establecer en la gestión de permisos el criterio de mínimos privilegios. Esto implica que, para que cada usuario pueda desempeñar sus funciones de una forma adecuada, se le asignará el menor número de privilegios para la realización de sus tareas. De esta forma, nos aseguraremos que, en caso de incidente, el impacto sea el mínimo posible.
Por otra parte, es muy importante realizar revisiones periódicas de los permisos asignados a cada empleado. Esto es debido a que, cada vez más, las empresas son dinámicas y los empleados se mueven internamente o entran y salen de la empresa. Para lo cual, lo más

recomendable es que los usuarios de las aplicaciones de negocio estén directamente asociados con los procesos de alta, baja y modificaciones de usuarios y permisos realizados por el Dpto. Recursos Humanos. De esta forma, nos aseguraremos que cualquier movimiento de un empleado en la Compañía, gestionado por el Dpto. Recursos Humanos, tiene su consecuencia directa en la gestión de sus permisos.

8.4.4.2 Actualizaciones de software

Con respecto a este apartado, en multitud de ocasiones, se han producido ciber-ataques debido a vulnerabilidades en los sistemas debido a que estos no se encontraban correctamente actualizados.
Por tanto, es muy crítico que, en nuestra Compañía, exista un proceso que mantenga actualizados nuestros sistemas.
En primer lugar, deberemos asegurarnos que el software que estamos utilizando sea fiable y corresponda con proveedores adecuados. Además, el responsable de este proceso deberá de estar pendiente y en contacto con estos proveedores, ya que, en algunos casos, estos proveedores sí que avisan de nuevas actualizaciones disponibles, pero, en otros casos no. También, en algunos casos, estos proveedores alertan de nuevas vulnerabilidades identificadas en su software.
En segundo lugar, será muy importante también, tener definido un proceso de parcheo y actualización de nuestros sistemas que tenga en cuenta los siguientes aspectos:

- Estas actualizaciones deberán ser realizadas en las ventanas temporales con menos impacto sobre la operativa diaria de la Compañía.
- Toda actualización deberá ser probada en un entorno diferente al de producción de nuestros sistemas, para evitar un impacto no deseado en ellos.

8.4.4.3 Contraseñas

Como una parte muy importante de la ciber-seguridad, son las contraseñas y la gestión de éstas. Será muy relevante establecer una política de contraseñas donde queden regulados ciertos criterios de la gestión de éstas para evitar el uso de contraseñas fáciles o débiles. Entre ellos:

- Antigüedad máxima y mínima de contraseñas
- Longitud mínima y complejidad de la contraseña
- Histórico de contraseñas
- Algoritmo de cifrado

8.4.4.4 Cuentas de usuarios

En primer lugar, comentar que cuando se adquieren ciertos dispositivos, aplicaciones, bases de datos, etc. suelen llevar asociados usuarios por defecto con contraseñas de fábrica

que son fácilmente adivinables. En este sentido, siempre que se adquiera un componente hardware o software, se deberán cambiar las claves de los usuarios por defecto.
Y, en segundo lugar, la Compañía deberá ser muy estricta con las cuentas de usuario que durante un periodo de tiempo dejen de utilizarse. Es decir, se deberá configurar de tal manera que, pasado un periodo de tiempo concreto, ésta se quedará inhabilitada. Y su posterior activación quedará a cargo del responsable de la misma o del responsable del área de negocio. De esta manera, se tendrán controladas todas las cuentas de usuario que no se encuentren activas.

8.4.4.5 Registros de eventos del sistema

Debido al número elevado de aplicaciones, bases de datos, etc., y la cantidad de usuarios que también suelen tener asociados, se generan números muy elevados de transacciones diariamente. Esto puede dar lugar a errores del sistema o incluso para la gestión de incidentes. Para lo cual, será crítico que todo el software que se considere reporte y registre sus eventos del sistema. En este caso, existen herramientas para la gestión de estos registros, de manera que, si al software o incluso al hardware quedara inaccesible, tendríamos disponibles los eventos registrados en un lugar independiente. También, existen herramientas parametrizables de análisis de eventos para que, en el caso que corresponda, nos avise mediante alarmas o avisos.

8.4.4.6 Copias de seguridad

La Compañía deberá desarrollar una política y procedimientos de la gestión de las copias de seguridad. Ya que, como ya se ha comentado anteriormente, en caso de incidente y que alguno de nuestros servicios se vea afectado de forma irreversible ocasionando pérdida de información, se podrá restablecer el servicio a través de las copias de seguridad.
La realización de las copias de seguridad, su contenido y su frecuencia, dependerá de la estrategia conjuntamente decidida entre las áreas de negocio de la Compañía y el área de IT, ya que la generación de copias de seguridad genera un almacenamiento de información elevado.
Además, algunas de las copias deberán ser externalizadas, es decir, almacenadas en ubicaciones diferentes a las instalaciones principales de la Compañía para que, en caso de incidente en las instalaciones, éstas copias externalizadas no se vean afectadas. Por otra parte, también, las copias de seguridad tienen que ser restauradas periódicamente con el objetivo de asegurarnos que se encuentran en perfecto estado para su restauración cuando sea necesario.

8.4.4.7 Cifrado de discos

En la mayoría de las Organizaciones, existen multitud de datos muy sensibles, desde las propias cifras financieras de la Compañía hasta información de empleados o clientes, con elevado grado de confidencialidad según la LOPD (*Ley Orgánica de Protección de Datos*).

En este sentido, existe la posibilidad de cifrar los discos duros de los ordenadores, aunque esta solución está más bien dirigida hacia los ordenadores portátiles y su posible extravío. Se da la posibilidad de cifrar aquellos portátiles de empleados que utilicen información muy sensible y que además tengan que salir de la Compañía. También, comentar que esta solución es costosa computacionalmente, por lo que puede acarrear ciertos inconvenientes.

8.4.4.8 Cifrado de las comunicaciones

Otro aspecto relevante de la seguridad es la información que enviamos hacia el exterior y también entre los empleados. Ya que, si ésta es enviada como texto plano, cualquier atacante que realice una escucha activa podrá leer lo que estamos enviando, así como abrir los archivos adjuntos. Por tanto, será importante cifrar las comunicaciones para evitar el robo de información.

8.4.5 Control de accesos y autenticación fuerte

Como ya se comentara anteriormente, en este aspecto, se seguirá el criterio de mínimos privilegios en cuanto a la asignación de permisos a usuarios.
En este sentido, es importante conocer los tres conceptos que intervienen en esta materia:

- Acceso: capacidad de hacer algo con recursos del ordenador. Se refiere en general a una capacidad técnica (por ejemplo, leer, crear, modificar o eliminar un archivo, ejecutar un programa, o el uso externo de conexión).
- Autorización: permiso para usar una computadora de recursos. Se concede el permiso, directa o indirectamente, por el propietario de la aplicación o sistema. El proceso de autorización en el acceso lógico a la información, es la verificación de que una persona conocida (autenticada) tiene la autoridad para acceder al sistema y para realizar la acción solicitada (login, lectura de un fichero, acceso a un dispositivo o recurso…).
- Autenticación: demostrar (en un grado razonable) que la entidad que solicita la conexión es quien dice ser.

Además, indicaremos a continuación algunos procedimientos y controles a implementar muy recomendables según los estándares, guías y normativas más relevantes:

- Deberán ser los Dptos. de negocio los que decidan los niveles de control de acceso a los recursos ya que son sus responsables los que conocen a su personal y su operativa diaria.
- Se deberá crear un procedimiento formal de Registro de Usuarios.
- La Gestión de Privilegios deberá estar restringida y controlada a través de un proceso formal de autorización.
- La Gestión de contraseñas de usuario deberá estar controlada por un procedimiento formalizado.
- Se deberán realizar periódicamente revisión de usuarios y permisos.
- Se deberán identificar los riesgos asociados al acceso de terceros a los recursos de la Compañía y la implantación de controles para la mitigación de estos.

- Se deberán controlar los accesos a la red de la Compañía tanto internamente como desde el exterior, vía acceso remoto.
- Se deberán configurar adecuadamente los puertos para evitar accesos no autorizados.
- Se deberán segmentar las redes de acuerdo a los resultados obtenidos del análisis de riesgos, identificando y aislando los activos más críticos.
- La Compañía se deberá asegurar que el acceso al código fuente de las aplicaciones y otros recursos se encuentra restringido únicamente al personal autorizado.
- Se deberán establecer políticas y procedimientos específicos para el adecuado uso de los portátiles y los dispositivos móviles que manejen o tengan acceso a información de la Compañía.

8.4.6 Seguridad en el ciclo de vida del desarrollo de los sistemas

En este apartado, se tratará la integración de la seguridad en el Ciclo de Vida del desarrollo de los sistemas de la Compañía. Esto será de aplicación tanto a recursos de desarrollo propio, como aquellos de adquisición comercial, como los que compartan ambas opciones, mixtos.

En este sentido, en primer lugar, recalcar la importancia de este apartado, debido a que cualquier cambio en los sistemas actuales o nueva implementación, podría tener graves repercusiones sobre el ecosistema de la Compañía si éste no es probado adecuadamente y ha seguido de forma fiel el Ciclo de Vida del desarrollo de los sistemas.

Inicialmente, a alto nivel, la Compañía deberá desarrollar una política para este efecto donde se desarrollen los procedimientos que apliquen en este proceso.

Para un mayor detalle en cuanto a la integración de la seguridad en el Ciclo de Vida, se puede consultar la Guía NIST 800-64 sobre las consideraciones de seguridad en el SDLC.

Este Ciclo de Vida deberá estar dividido en las siguientes fases:

- Iniciación
- Desarrollo/Adquisición (*en el caso de la solución comercial*)
- Implementación/Evaluación
- Operación/Mantenimiento
- Eliminación

En la Política anteriormente mencionada, se deberán describir los roles y las responsabilidades de cada uno de los participantes en este ciclo. También, en esta Política, se indicarán los procedimientos específicos de cada una de las partes de este proceso.

Una vez establecidos los roles y las fases, indicaremos los aspectos y consideraciones a tener en cuenta dentro del proceso.

Como primer punto, antes del desarrollo o la adquisición comercial, se deberá debatir el objetivo y los requisitos a cumplir por esta nueva solución. Para lo cual, deberán participar

todos los responsables, desde el área de negocio solicitante hasta el Dpto. IT para los requerimientos o el Dpto. Auditoría Interna.
En este punto, deberán quedar muy claros los objetivos y necesidades que justifiquen el nuevo desarrollo o recurso. También, una vez definidos estos, el Dpto. IT deberá describir específicamente los requerimientos de seguridad a aplicar, junto con el Dpto. Auditoría Interna, quien deberá velar también por la calidad del producto.
Una vez definido esto, se deberá dejar por escrito la solicitud de desarrollo o compra por parte del responsable del Dpto. solicitante, quedando como registro. En el cual, se deberán incluir todos los detalles para su desarrollo o adquisición, así como la fecha para la cual se necesita disponer del recurso.

Después de esto, en el caso de ser un desarrollo propio de la Compañía, y habiendo descrito las necesidades y requisitos, el equipo de desarrolladores procederá con el desarrollo inicial. En esta fase, serán muy importante el establecimiento de algunos controles de seguridad integrados en este sub-proceso. Como son:

- El desarrollo se realizará en un entorno diferenciado del entorno de producción.
- El acceso al código fuente que se va a desarrollar será de acceso únicamente a las personas que autorizadas.
- Se deberán determinar los recursos necesarios para poder llevar a cabo este desarrollo.
- Se deberán establecer los riesgos que se asumen para su desarrollo, ya sea de impacto en el negocio o en los sistemas, de recursos, etc.
- Se deberá guardar un registro de versiones del código fuente, así como también copias de seguridad de las distintas fases.
- Se deberá tener activado el registro de auditoría para que, en caso de error o incidente, se pueda averiguar el usuario y momento del mismo.

Una vez se haya desarrollado el código fuente, pasaremos a ejecutar las pruebas pertinentes y evaluar el resultado obtenido. En este paso, será relevante también tener en cuenta las siguientes consideraciones:

- Las pruebas deberán ser realizadas en un entorno diferente al entorno de producción.
- Las personas que realizarán las pruebas deberán ser diferentes de las personas que hayan desarrollado el código fuente.
- Para un mayor aprovechamiento de esta fase, y asegurarse que el nuevo desarrollo cumple con las necesidades y requisitos pre-definidos, será muy conveniente que participe en esta fase el responsable que solicitó el nuevo desarrollo. Y, de esta forma, nos aseguraremos que el nuevo desarrollo cumple con todas las funcionalidades requeridas.
- Las pruebas deberán ser realizadas con copias de información del entorno productivo de cara a ser un fiel reflejo a cómo funcionaría la nueva herramienta en ese entorno.
- Todas las pruebas deberán quedar documentadas, incluyendo sobre todo los resultados de éstas, éxito o fallo.
- Como parte de estas pruebas, también no sólo estarán las pruebas de validación de usuario ya comentadas, sino las pruebas que deberán llevarse a cabo de integración

con los sistemas de la Compañía. Aspecto muy crítico debido a la posibilidad de incompatibilidades entre ellas.
- Los responsables de IT y Auditoría Interna deberán llevar a cabo validaciones que aseguren unos criterios mínimos de calidad.
- En este apartado, y con la ayuda del responsable de negocio, se llevará a cabo la configuración de la nueva herramienta. En este punto, también deberán participar los responsables de IT y de Auditoría Interna para definir e implementar la configuración de seguridad de la herramienta.

Y, como última fase, en el caso que corresponda, la eliminación que garantiza el cese ordenado del sistema, almacenar la información necesaria apropiadamente para su posterior migración a la nueva herramienta o bien porque requerimientos o normativas legales que exigen su custodia posterior. Se deberán tener las siguientes consideraciones:

- Se deberá desarrollar un Plan de Eliminación/Transición
- Adecuado archivo de la información crítica
- Se deberán limpiar adecuadamente los soportes de almacenamiento
- Se deberá borrar adecuadamente el software y eliminar el hardware si así se considera.

En el caso de que se trate de una adquisición comercial, esta fase será muy parecida en cuanto a las consideraciones ya comentadas, debido a que principalmente se deberán realizar también las validaciones de usuario y las pruebas de integración con los sistemas.

En la siguiente fase, se procede a la subida a producción. Esta fase se llevará a cabo en el caso de que las anteriores hayan finalizado con éxito. Se deberán tener en cuenta las siguientes consideraciones:

- El personal que realice la subida al entorno de producción deberá ser completamente diferente al personal que ha ejecutado las fases anteriores.
- Se deberá realizar la subida a producción en el momento que menor impacto tenga sobre la operativa diaria de la Compañía.
- Una vez realizada la subida a producción, se deberán realizar pruebas para asegurar que el desarrollo se ajusta a lo validado en el entorno de pruebas.
- Se deberá completar y finalizar toda la documentación generada durante el proceso para su archivo y custodia posterior.
- Se realizará un seguimiento del funcionamiento de la herramienta, manteniendo un contacto constante con los usuarios de negocio que la vayan a utilizar.

8.4.7 Protección frente al malware

El malware es un programa que se instala en nuestro sistema operativo, con el objetivo de corromper la confidencialidad, integridad o disponibilidad de la información almacenada en el sistema.
En nuestra Compañía, se deberán dedicar esfuerzos específicos para la prevención de este tipo de ataques cada más comunes hoy en día. Estos esfuerzos además deberán ir dirigidos y promovidos desde la Dirección mediante políticas y concienciación de los empleados,

hasta procedimientos operativos a implantar en la operativa diaria de los empleados a través de la implementación de controles, como por ejemplo software de detección de malware o cortafuegos. Y, a pesar de estos esfuerzos, este tipo de ataques se seguirán produciendo, para lo cual, la Compañía también deberá tener desarrollados procedimientos de restauración de los daños ante este tipo de ataques, mediante una adecuada gestión de incidentes.

Los elementos principales para que nuestra Compañía pueda protegerse y prevenir este tipo de ataques son:

- Políticas
- Concienciación
- Minimización de vulnerabilidades
- Minimización de amenazas
- Planes de gestión de crisis

Con respecto a la política, es relevante que exista una política, pudiendo ser específica de este tema o que se incluya dentro de otra, pero que trate este tema haciendo mención a los procedimientos específicos que se deben llevar a cabo, así como a la concienciación de los empleados en esta materia. Como, por ejemplo, se detallan a continuación algunas consideraciones a incluir:

- Todo dispositivo externo que se conecte a un sistema de la Compañía deberá ser escaneado en busca de malware previamente a su uso.
- En el uso del correo electrónico, se limitarán y censurarán los archivos comprimidos, ejecutables, etc. analizándolos siempre previamente a su ejecución.
- Se limitará el acceso de los empleados a otras redes externas a la Compañía.
- Todos los dispositivos de la Compañía contendrán siempre el mismo paquete de software antivirus y se asegurará que éste siempre se encuentre actualizado.

En lo relativo a la concienciación de los empleados, se divide en la parte proactiva y en la parte reactiva. En primer punto, hace referencia a la concienciación a los empleados de las formas que suelen utilizar los hackers para el acceso a los sistemas de la Compañía. Como, por ejemplo:

- A través de archivos adjuntos desde destinatarios desconocidos
- Solicitud de información personal o financiera de la Compañía desde destinatarios conocidos
- Los empleados a veces desactivan las medidas de seguridad implementadas en los sistemas de la Compañía.
- También, debería de estar prohibido y restringido la descarga e instalación de software externo de la Compañía en los sistemas del usuario.

Y, en segundo lugar, se encontraría la concienciación reactiva. Esto se refiere a enseñar a los empleados a cómo tienen que reaccionar ante un ataque. Tanto si éste aún no se ha producido, pero se están cumpliendo algunas de las consideraciones indicadas anteriormente, como si el ataque ya se está produciendo. En estos casos, se indicará en detalle cómo tiene que reaccionar el empleado, a quién tiene que avisar y qué acciones tiene que llevar a cabo para, al menos, intentar minimizar el impacto producido por el ataque.

Con respecto a la minimización de vulnerabilidades, la mayoría proceden de sistemas no actualizados adecuadamente, ya sea un sistema operativo, una base de datos o un propio antivirus. Y es que puede ser que el cliente aun no haya instalado el parche del proveedor o que el proveedor no haya identificado la vulnerabilidad o no la haya comunicado a sus clientes.
Son estos casos, los que son aprovechados por los hackers para introducirse en las redes de las Compañías.
Para esto, sobre todo conviene tener actualizados todos los sistemas de la Compañía, ya sea a través de las actualizaciones automáticas o bien consultando periódicamente diferentes fuentes como las de nuestros proveedores de software de antivirus o también los boletines que publica periódicamente el CERT. Además, se recomienda tener en cuenta las siguientes consideraciones:

- Disponer de un procedimiento formalizado de gestión de parches y actualizaciones.
- Previo a la instalación de cualquier parche o actualización en el entorno productivo, estos deberán ser probados en un entorno diferente sin impacto en el entorno productivo.
- Requerir siempre la autenticación para el acceso a cualquier red de nuestra Compañía.

Además de la minimización de vulnerabilidades, existe otra opción muy recomendable a las empresas que es la utilización de software específico para la detección de malware. Entre los que destacan:

- Software antivirus
    - Escaneado de componentes críticos del sistema
    - Actividades de monitorización en tiempo real
    - Verificación del correcto funcionamiento de las aplicaciones de la Compañía
    - Identificación y análisis de archivos de virus conocidos
- Software de identificación y eliminación de spyware
    - Seguimiento específico al comportamiento de ciertas aplicaciones
    - Exploraciones periódicas y aleatorias de recursos
    - Monitorización de los controladores de red
    - Prevenir la carga automática de ciertos archivos al arranque de los sistemas o las propias cookies
- IPS (*Sistema de Prevención de Intrusiones*)
    - Se trata de una forma proactiva de defensa ante ciber-ataques basada en el análisis de paquetes del tráfico de red antes de que estos lleguen a su destino. Esto evita muchos ataques ya que estos son identificados antes de materializarse.

Por último, se indicarán a continuación una serie de consideraciones a aplicar por parte de las Organizaciones:

- La Compañía deberá intentar minimizar los daños después de un ataque de malware
- También deberá promover políticas que apoyen la prevención de ataques de malware

- A través de políticas y procedimientos, se deberán disponer de métodos de respuesta rápida ante incidentes:
    - Preparación
    - Detección y análisis
    - Contención
    - Actividad posterior al incidente

8.4.8 Gestión de registros

Una parte fundamental de la seguridad integrada en los procesos operativos de las Organizaciones es la generación y adecuada gestión de registros de actividad.
Por una parte, de cara a la gestión de incidentes y análisis posterior, será clave la generación de registros para averiguar el origen del incidente, quién lo originó, por dónde accedió a la red, etc., es decir, una serie de pistas que ayudarán a la Compañía.
Y, por otra parte, de cara a la optimización de recursos, los registros de actividad ayudan a las Compañías a identificar los errores que se producen en sus sistemas y el motivo por el que se están generando, ayudando a su investigación.

Los tipos de registros de actividad que se suelen generar son:

- De software de seguridad (anti-spyware, anti-malware, etc.)
- De acceso remoto (VPN)
- De autenticación
- De dispositivos de comunicaciones (configuración de routers)
- Etc.

Para una adecuada gestión de estos registros generados por los sistemas de la Compañía, se recomienda utilizar y centralizar los registros de los sistemas en herramientas desarrolladas específicamente para tal efecto. Decidiendo, en primer lugar, qué registros le interesa a la Compañía almacenar. Para, posteriormente, clasificar y priorizar, de tal manera, que se puedan aprovechar en muchos casos como avisos o alarmas de incidentes.

Para llevar a cabo este proceso, es recomendable desarrollar políticas y procedimientos que definan roles y responsabilidades dentro de la Compañía.

8.5 Gestión de incidentes

En este apartado, destacar que, teniendo en cuenta el número de ciber-ataques que diariamente se producen y continúan aumentando, se considera imprescindible que las Organizaciones dispongan de un proceso formalizado de Gestión de Incidentes. En este sentido, en primer lugar, se definirá una política donde se describa a alto nivel lo que

considera la Organización como incidente, la escala de valoración de incidentes, así como los procedimientos, los roles y los responsables de estas tareas.

Algunos de los ciber-incidentes más comunes serían:

- Denegación de Servicio
- Código malicioso
- Acceso no autorizado
- Uso inapropiado de recursos de la Compañía

Además, esta política deberá estar aprobada por la Alta Dirección de la Compañía e indicará cómo se comunica con el resto de empleados.

Después, a partir de los procedimientos desarrollados, se establecerá una estrategia de actuación sobre cada uno de los ciber-incidentes clasificados, así como las tareas que tendrá que desempeñar cada uno de los componentes que participen en el Equipo de Respuesta ante ciber-incidentes.

A continuación, se recomiendan los siguientes pasos a seguir:

1. Se realizará una comunicación a todos los empleados
2. Se analizarán las pruebas recopiladas
3. Se notificará a las personas responsables que forman parte del Equipo de Respuesta ante ciber-incidentes, así como a la Alta Dirección
4. Se notificará al CNPIC
5. Se procederá a la detención del incidente
6. Se preservarán las pruebas
7. Se limpiarán todos los recursos infectados
8. Se identificarán todas las vulnerabilidades que fueron explotadas
9. Se restaurarán las operaciones en los sistemas
10. Se generará un informe final

9 Conclusiones

9.1 Conclusiones

Después de la revisión realizada en este proyecto, los ataques que se han mencionado y que, a día de hoy, siguen ocurriendo, se podría decir que las principales causas de que estos ataques se sigan materializando, se debe a la falta de formación y concienciación de los empleados de las propias empresas atacadas y del ciudadano en general. Ya que la mayoría de estos ataques se deben a vulnerabilidades generadas por el ser humano y aprovechadas por los hackers. También, hay que destacar la poca importancia que, aun a día de hoy, las empresas, medianas, pequeñas y grandes, dan a la ciberseguridad y las graves consecuencias que, en cuestión de segundos pueden llegar a tener.

Una vez incrementada esa relevancia de la ciberseguridad con este documento, planteo el objetivo de este proyecto como una forma de proveer a pequeñas y medianas organizaciones de una guía práctica para la protección de sus infraestructuras críticas ante ciber-ataques. A través de esta guía, podrá acometer con un gran nivel de detalle las exigencias definidas por los organismos nacionales a nivel de seguridad de la información.
Además, para poner en valor el trabajo y el riesgo que las infraestructuras críticas tienen asociado, se han detallado y referenciado varios ejemplos que reflejan las consecuencias que pueden tener lugar en el caso de que, si el ciber-ataque se produce, nuestra organización no esté preparada.

Por otra parte, cabe indicar que, el seguimiento de esta guía supone un reto complejo para cualquier organización ya que requiere un nivel de madurez elevado en términos de seguridad de la información. Lo cual puede conllevar elevados costes en cuanto a tecnología, así como personal específico implicado y definición y/o modificación de procesos y políticas internas de la organización.

Referencias

[1] http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html (*consultada el día 30/05/2017*)

[2] https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf (*consultada el día 30/05/2017*)

[3] http://www.rtve.es/noticias/20160217/espana-sufrio-134-ciberataques-infraestructuras-criticas-2015/1303205.shtml (*consultada el día 30/05/2017*)

[4] https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf (*consultada el día 30/05/2017*)

[5] http://www.bbc.com/mundo/internacional/2010/09/100926_virus_stuxnet_iran_planta_nuclear_aw.shtml (*consultada el día 30/05/2017*)

[6] http://cnnespanol.cnn.com/2015/05/18/fbi-hacker-dice-que-logro-controlar-el-motor-de-un-avion-durante-un-vuelo/ (*consultada el día 30/05/2017*)

[7] http://tecnologia.elpais.com/tecnologia/2016/11/22/actualidad/1479829002_717742.html (*consultada el día 30/05/2017*)

[8] http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas-/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/seguridad-y-ciudadania. Revista del Ministerio del Interior – Seguridad y Ciudadanía – 2014. (*consultada el día 30/05/2017*)

[9] http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas-/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/seguridad-y-ciudadania. Revista del Ministerio del Interior – Seguridad y Ciudadanía – 2015. (*consultada el día 30/05/2017*)

[10] https://www.aeiciberseguridad.es/index.php (*consultada el día 30/05/2017*)

[11] CNPIC, "Guía de Buenas Prácticas Plan de Protección Específico (PPE)" http://www.cnpic.es/Biblioteca/Noticias/GUIA_BUENAS_PRACTICAS_PPE.pdf (*consultada el día 30/05/2017*)

[12] CNPIC, "Guía de Buenas Prácticas Plan de Seguridad del Operador (PSO)" https://www.grupocontrol.com/sites/default/files/Gu%C3%ADa%20de%20Buenas%20Pr%C3%A1cticas%20PSO.pdf (*consultada el día 30/05/2017*)

[13] Gobierno de España, "Estrategia de seguridad nacional" http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional (*consultada el día 30/05/2017*)

[14] Boletín Oficial del Estado, "Resolución del 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos" http://www.boe.es/buscar/doc.php?id=BOE-A-2015-10060 (*consultada el día 30/05/2017*)

[15] MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administración Española https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WS3d59zta1s (*consultada el día 30/05/2017*)

[16] NORMAS UNE: UNE-71501-1, UNE-71501-2, UNE-71501-3 y UNE-71504 en relación al análisis de riesgos de sistemas de información;

http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0025819#.WS3eJNzta1s (*consultada el día 30/05/2017*)

[17] ISO/IEC 27001, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información https://www.iso.org/standard/54534.html (*consultada el día 30/05/2017*)

[18] ISO/IEC 27005, Information Technology. Security Techniques. Information Security Risk Management. https://www.iso.org/standard/54534.html (*consultada el día 30/05/2017*)

[19] ISO/IEC 27006, Information Technology. Security Techniques. Requirements for bodies Providing Audit and Certification of Information Security Managements Systems https://www.iso.org/standard/54534.html (*consultada el día 30/05/2017*)

[20] NIST 800-83 Guide to Malware Incident Prevention and Handling http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf (*consultada el día 30/05/2017*)

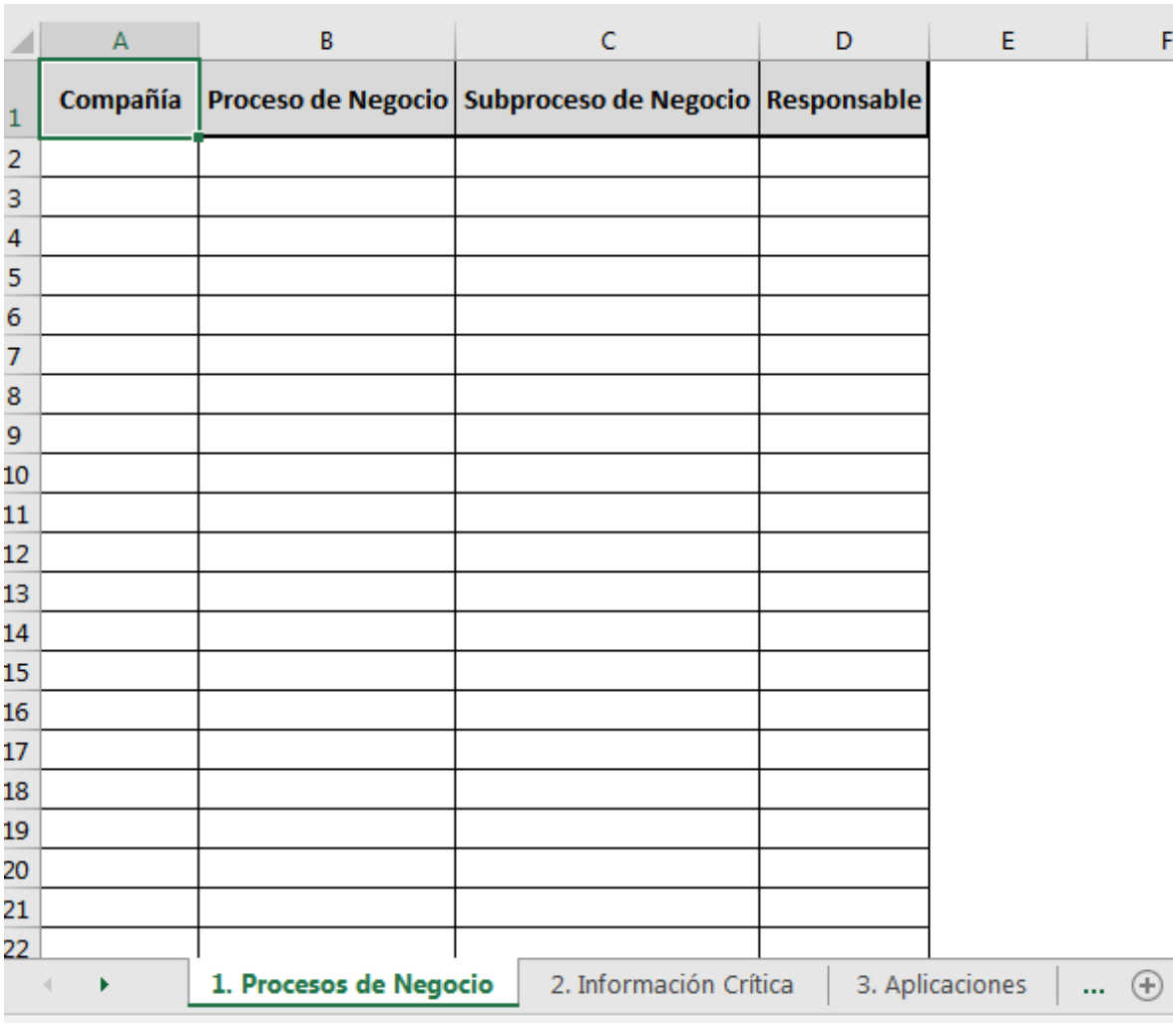
[21] NIST 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf (*consultada el día 30/05/2017*)

Glosario

ARLI-CIB	Análisis de Riesgos Ligero de Ciberseguridad
ARLI-SI	Análisis de Riesgos Ligero de Seguridad Integral
C4V	Construcción de Capacidades de Ciberseguridad de la Cadena de Valor
CERT	Computer Emergency Response Team
CERTSI	CERT de Seguridad e Industria
CNPIC	Centro Nacional para la Protección de las Infraestructuras Críticas
ENSI	Esquema Nacional de Seguridad Industrial
IEC	International Electrotechnical Commission
IMC	Indicadores para la Mejora de la Ciberresiliencia
INCIBE	Instituto Nacional de Ciberseguridad
ISA	International Society for Automation
OC	Operador Crítico
PES	Plan Estratégico Sectorial
PIC	Protección de Infraestructuras Críticas
SCI	Sistema de Control Industrial
SES	Secretaría de Estado de Seguridad

Anexo

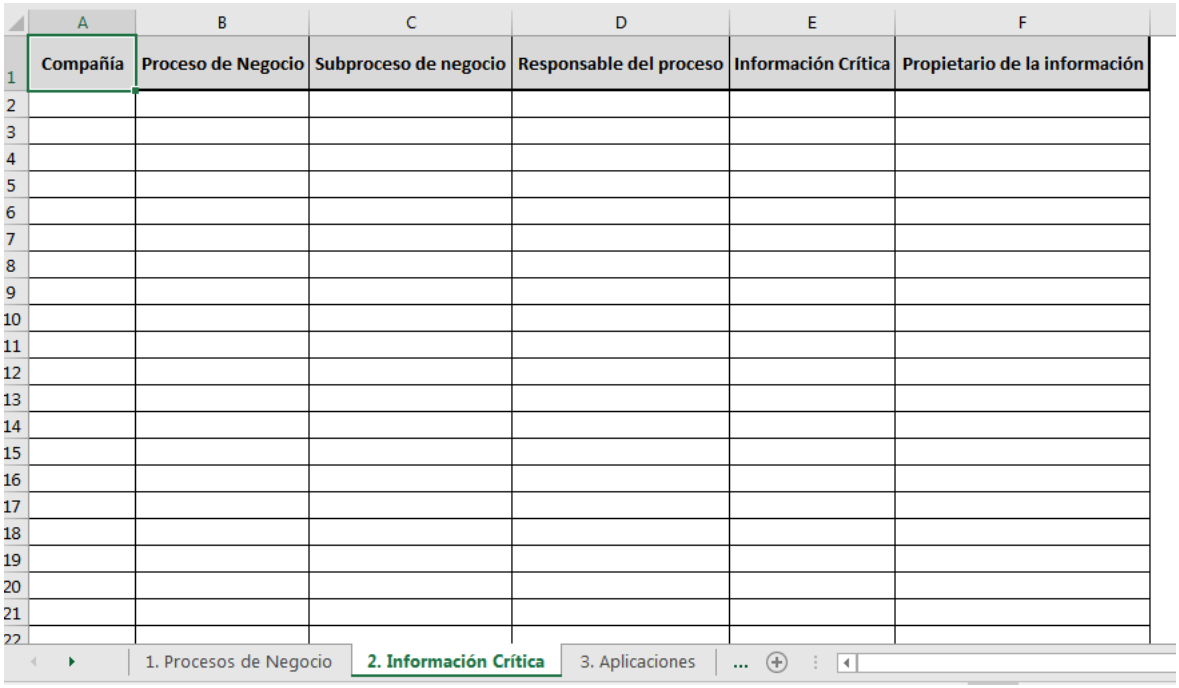
9.1 Identificación y clasificación de activos



	A	B	C	D	E	F
1	**Compañía**	**Proceso de Negocio**	**Subproceso de Negocio**	**Responsable**		
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

1. Procesos de Negocio | 2. Información Crítica | 3. Aplicaciones | ...

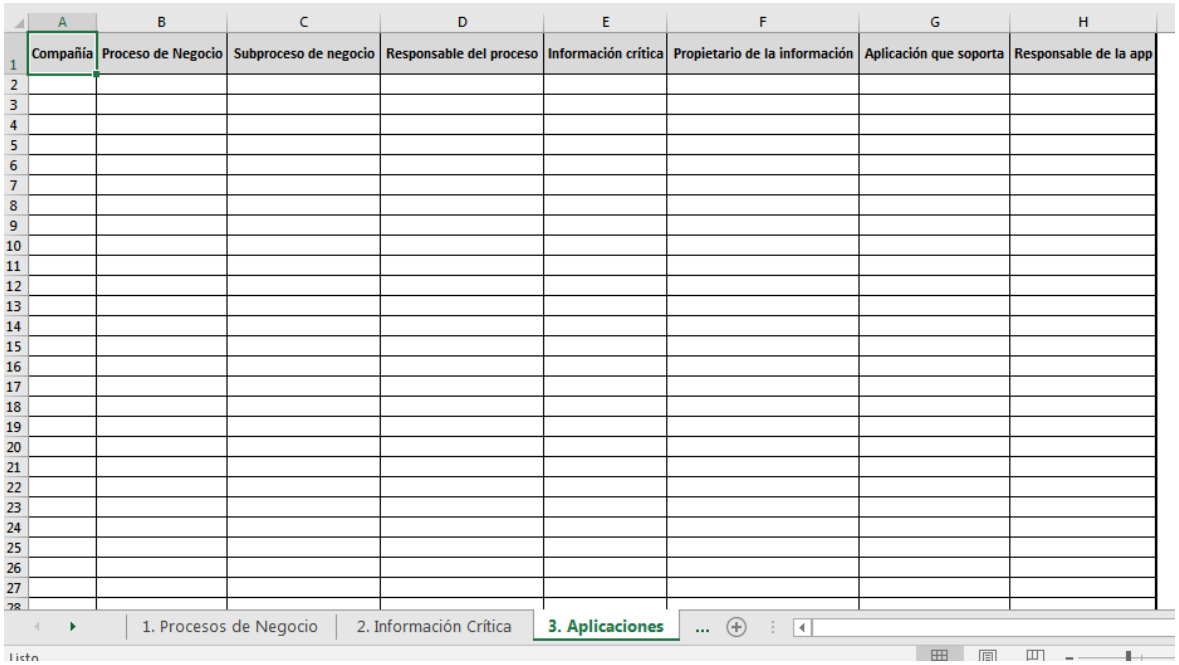
Nivel: Información crítica:



Compañía	Proceso de Negocio	Subproceso de negocio	Responsable del proceso	Información Crítica	Propietario de la información

1. Procesos de Negocio | 2. Información Crítica | 3. Aplicaciones

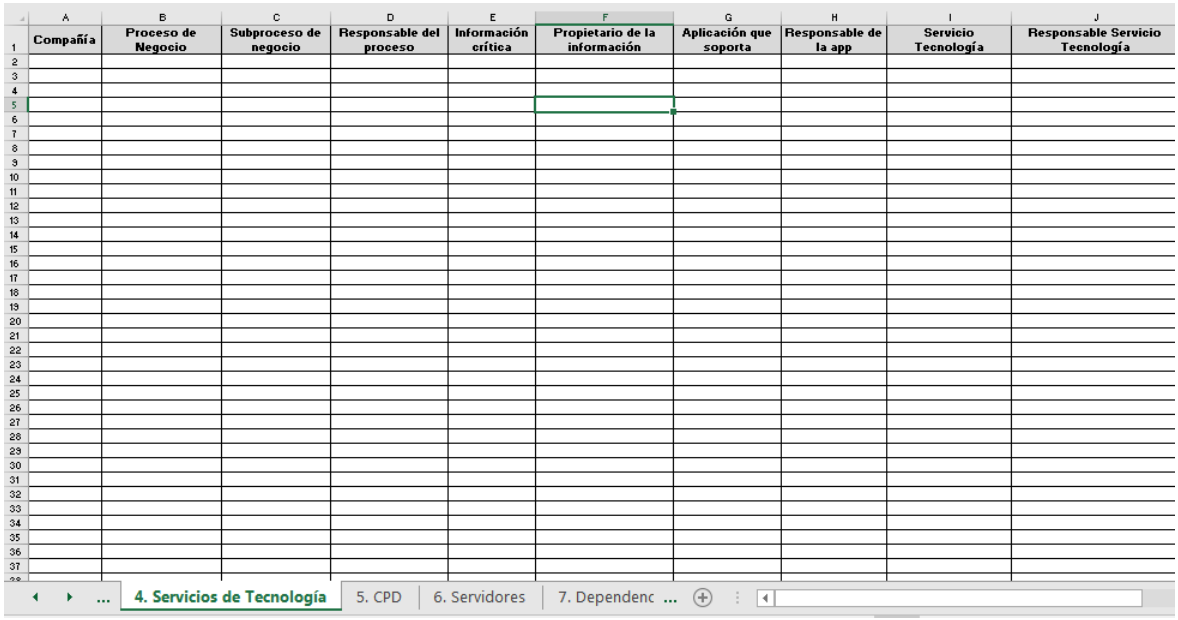
Nivel: Aplicaciones



Compañía	Proceso de Negocio	Subproceso de negocio	Responsable del proceso	Información crítica	Propietario de la información	Aplicación que soporta	Responsable de la app

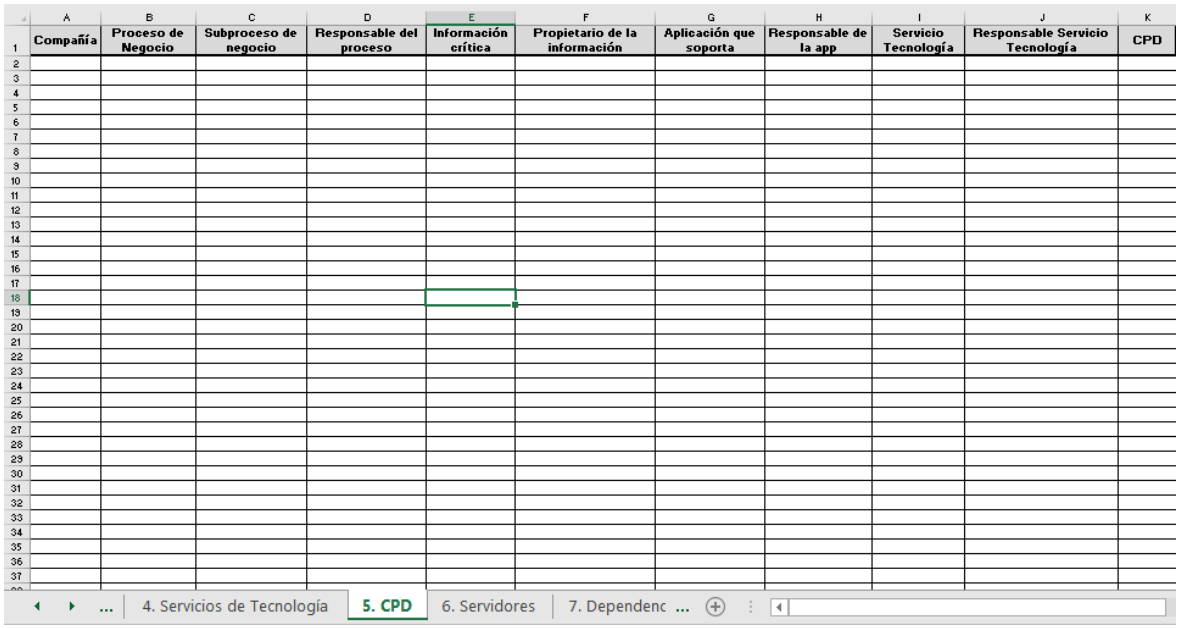
1. Procesos de Negocio | 2. Información Crítica | 3. Aplicaciones

Nivel: Servicios de Tecnología



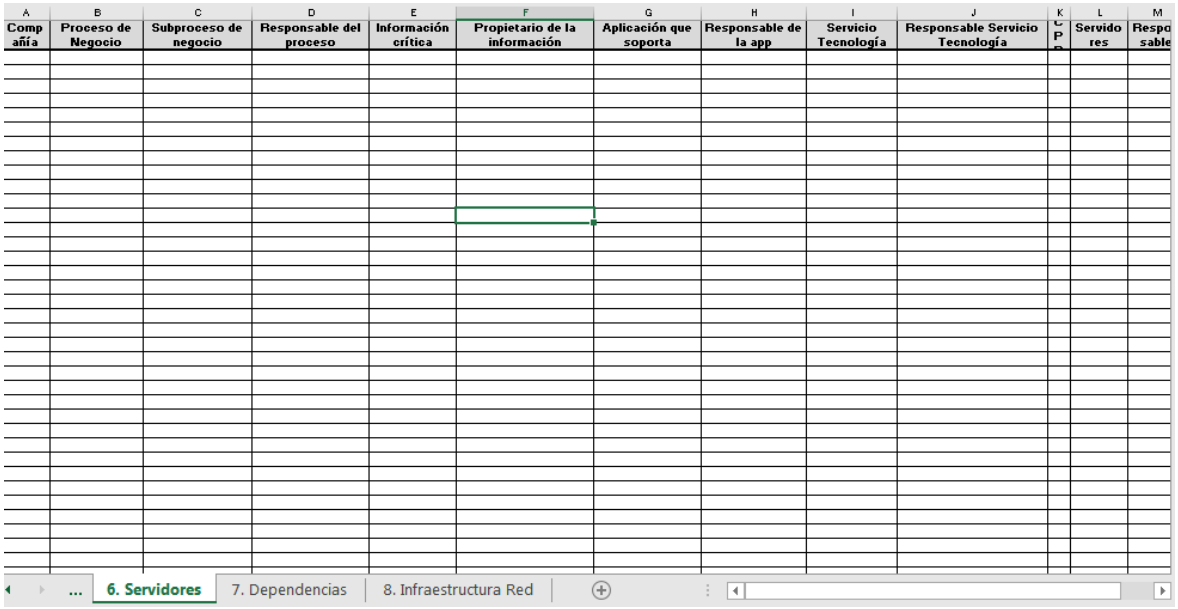
	A	B	C	D	E	F	G	H	I	J
1	Compañía	Proceso de Negocio	Subproceso de negocio	Responsable del proceso	Información crítica	Propietario de la información	Aplicación que soporta	Responsable de la app	Servicio Tecnología	Responsable Servicio Tecnología

Nivel CPD (*Centro de Procesamiento de Datos*)



	A	B	C	D	E	F	G	H	I	J	K
1	Compañía	Proceso de Negocio	Subproceso de negocio	Responsable del proceso	Información crítica	Propietario de la información	Aplicación que soporta	Responsable de la app	Servicio Tecnología	Responsable Servicio Tecnología	CPD

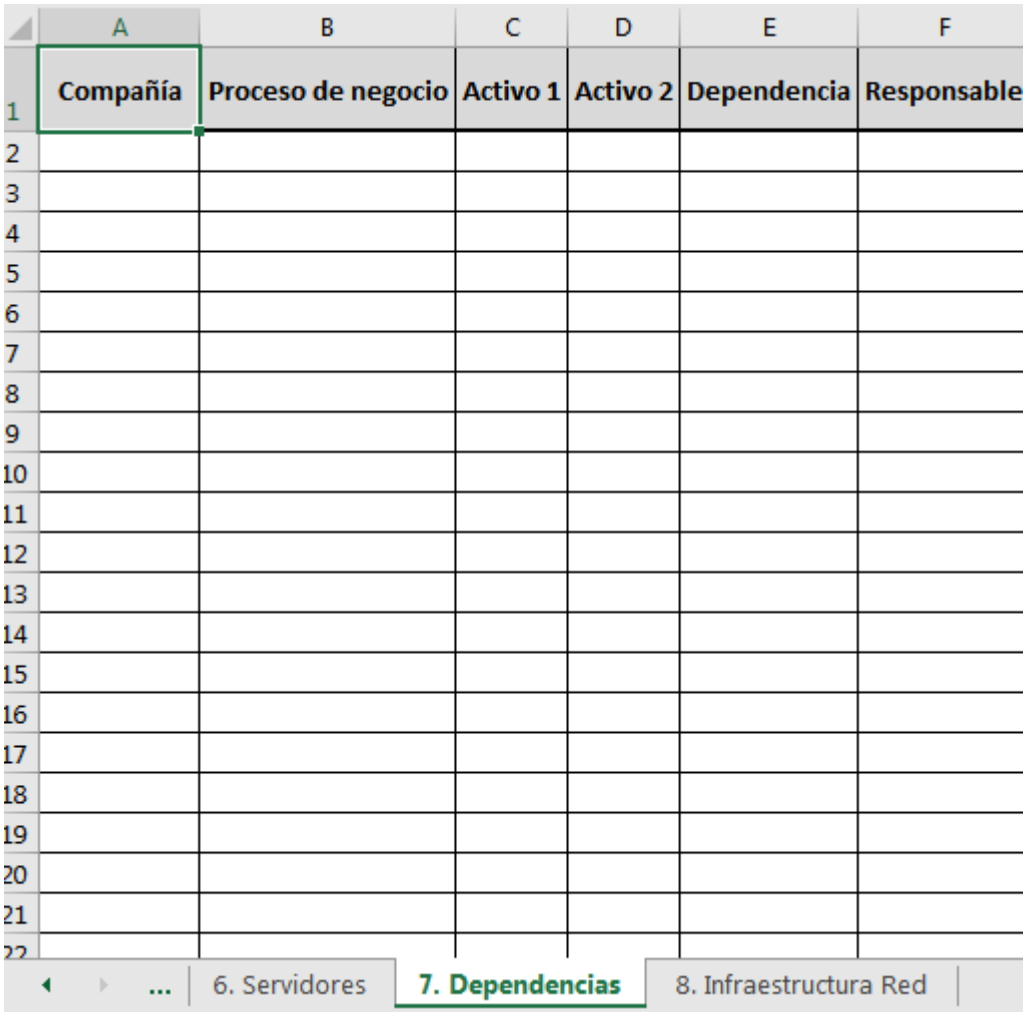
Nivel: Servidores



A	B	C	D	E	F	G	H	I	J	K	L	M
Compañía	Proceso de Negocio	Subproceso de negocio	Responsable del proceso	Información crítica	Propietario de la información	Aplicación que soporta	Responsable de la app	Servicio Tecnología	Responsable Servicio Tecnología	CPD	Servidores	Responsable

... | 6. Servidores | 7. Dependencias | 8. Infraestructura Red

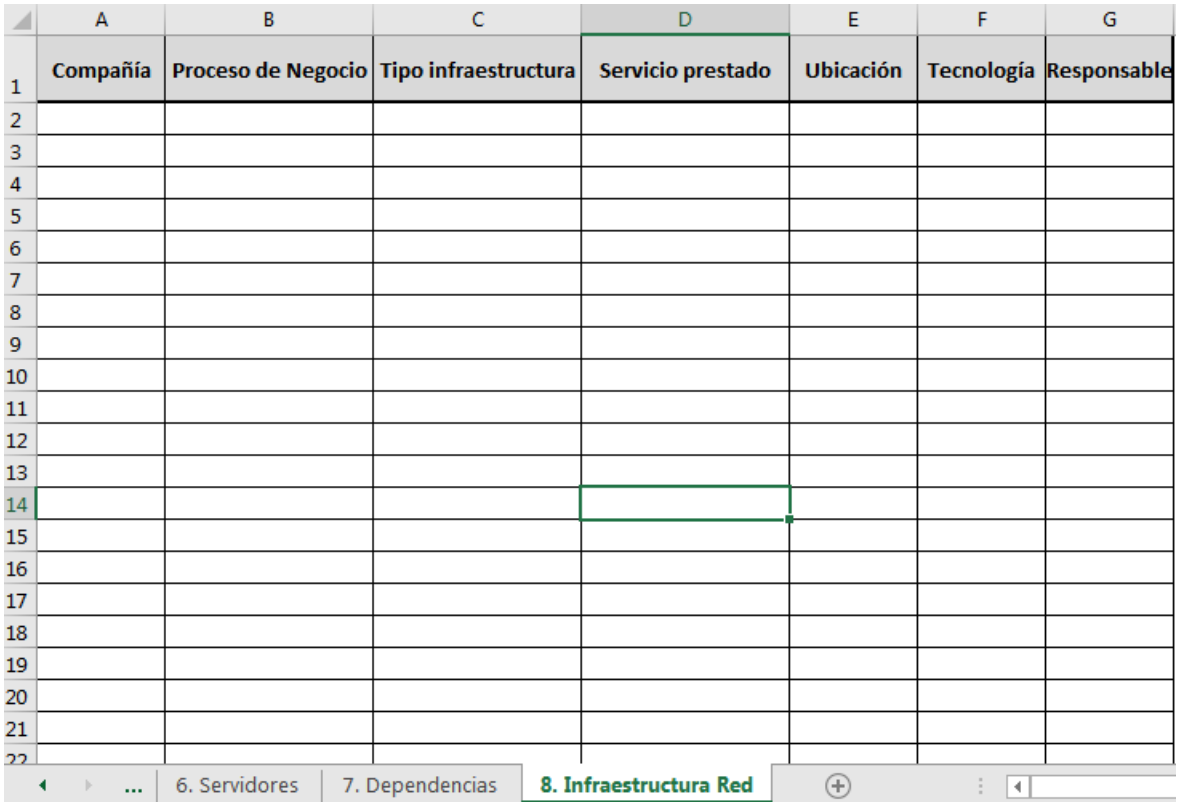
Nivel: Dependencias entre activos



	A	B	C	D	E	F
1	Compañía	Proceso de negocio	Activo 1	Activo 2	Dependencia	Responsable
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						

... | 6. Servidores | 7. Dependencias | 8. Infraestructura Red

Nivel: Infraestructura de Red



9.2 Presupuesto

A continuación, se ha realizado una estimación del coste que le supondría a una Compañía el seguimiento de esta Guía. Se ha supuesto lo siguiente:

- 1500-5000 empleados
- CPD Principal y Secundario
- Sistemas redundantes
- ERP como sistema informacional

Para ello, se supondrá el caso de la contratación de los servicios proporcionados por una empresa externa que ayude en la implementación de esta guía.

Se ha supuesto la contratación del siguiente grupo de trabajo:

- Gerente del proyecto
- Jefe de equipo con experiencia en seguridad de la información
- Dos consultores de seguridad de la información

Y un coste asociado por persona de:

- Gerente: 500 € / hora
- Jefe de equipo: 250 € / hora
- Dos consultores: 200 € / hora

Para llevar a cabo el proyecto de una forma adecuada y completa, se ha estimado una duración de 6 meses de ejecución del proyecto para una empresa media de 1000-5000 empleados.

Y la participación de los componentes del grupo de trabajo será de:

- Gerente: 192h (24 jornadas)
- Jefe de equipo: 480h (60 jornadas)
- Dos consultores: 1920h (240 jornadas)

Resultando un coste total del proyecto de: **408.000 €**.

Las fases y tareas del proyecto quedarían definidas de la siguiente manera:

Actividad	Personal implicado	Posibilidad de implementar una plataforma	Número de jornadas
Kick-off	• Gerente • Jefe de equipo • Consultores	No	1
Identificación y clasificación de activos	Responsables de todas las áreas implicadas (10)	Sí	30
Valoración de los activos	Responsables de todas las áreas implicadas (10)	Sí	15
Identificación de las amenazas	Responsable de Seguridad	Sí	10
Identificación de los impactos	Responsable de Seguridad	Sí	10
Valoración del riesgo	Responsable de Seguridad	Sí	15
Identificación de medidas de seguridad a implantar	Responsable de Seguridad y Responsable de IT	Sí	10
Adquisición y/o modificación de medidas de seguridad	Responsables de: Seguridad, IT y Compras		5
Validación de las medidas	Responsable de Seguridad y Responsable de IT		14
Revisión del cumplimiento con los requisitos PPE, PSO	Responsable de Seguridad		10

Madrid, Junio de 2017

El Ingeniero Jefe de Proyecto

Fdo.: Alberto Menchén Atienza
Ingeniero de Telecomunicación

9.3 Pliego de Condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de una Guía para la Protección de las Infraestructuras Críticas ante Ciberataques. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de

obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad "Presupuesto de Ejecución de Contrata" y anteriormente llamado" Presupuesto de Ejecución Material" que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones, así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.