Implantación de un SGSI en la empresa

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza2

INDICE

CAPÍTULO 1 – Conceptos básicos sobre Seguridad de la Información.

Hola. Mi nombre es Raúl. Trabajo como Técnico de Seguridad en INTECO, el Instituto Nacional de Tecnologías de la Comunicación.

En INTECO trabajamos para fomentar e impulsar la seguridad de la información y su implantación en las empresas y organizaciones. A diario, estamos amenazados por riesgos que ponen en peligro la integridad de nuestra información y con ello la viabilidad de nuestros negocios. Riesgos que provienen no sólo desde el exterior de nuestras empresas, sino también desde el interior.

Para poder trabajar en un entorno como este de forma segura, las empresas pueden asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información.

A lo largo de los próximos minutos, voy a detallarte las ventajas de implantar este sistema en tu empresa y cómo hacerlo.

Podríamos definir un Sistema de Gestión de Seguridad de la Información como una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa.

Quizá oigas hablar de este sistema por sus siglas en español, SGSI, o por sus siglas en inglés, ISMS.

Antes de comenzar a ver las características de este tipo de sistemas, es importante diferenciar entre seguridad informática y seguridad de la información.

La primera, la seguridad informática, se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio.

Mientras que la seguridad de la información, se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización.

Entre los muchos ejemplos de información que podemos encontrar en nuestra empresa están los correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos y un largo etcétera.

Al identificar los activos de información tenemos que tener en cuenta que estos pueden proceder de distintas fuentes de información dentro de la empresa y que pueden encontrarse en diferentes

soportes, como papel o medios digitales. Además, es necesario considerar el ciclo de vida de la información, ya que lo que hoy puede ser crítico para nuestro negocio puede dejar de tener importancia con el tiempo.

Como hemos visto con anterioridad, para garantizar la seguridad de toda esta información podemos contar con la ayuda de un Sistema de Gestión de Seguridad de la Información.

Esta metodología nos va a permitir, en primer lugar, analizar y ordenar la estructura de los sistemas de información.

En segundo lugar, nos facilitará la definición de procedimientos de trabajo para mantener su seguridad.

Y por último, nos ofrecerá la posibilidad de disponer de controles que permitan medir la eficacia de las medidas tomadas.

Estas acciones van a proteger a nuestra organización frente a amenazas y riesgos que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de negocio.

De esta manera conseguiremos mantener el riesgo para nuestra información por debajo del nivel asumible por la propia organización.

La gestión de los riesgos a través de un Sistema de Gestión de Seguridad de la Información nos va a permitir preservar la confidencialidad, integridad y disponibilidad de la misma, en el interior de la empresa, ante nuestros clientes y ante las distintas partes interesadas en nuestro negocio.

La confidencialidad implica el acceso a la información por parte únicamente de quienes están autorizados.

La integridad conlleva el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Y la disponibilidad entraña el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran.

El acrónimo utilizado para hablar de estos parámetros básicos de la seguridad de la información es CID en español y CIA en inglés.

Con el fin de proporcionar un marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000.

Estas normas nos van a permitir disminuir de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal.

Más adelante analizaremos con detalle estas normas.

CAPÍTULO 2 – La seguridad y su justificación desde el punto de vista del negocio.

La información es un valioso activo del que depende el buen funcionamiento de una organización. Mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de negocio.

Por esa razón, desde tiempos inmemorables las organizaciones han puesto los medios necesarios para evitar el robo y manipulación de sus datos confidenciales.

En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que ha aumentado los riesgos para las empresas que se exponen a nuevas amenazas.

Desafortunadamente, es relativamente fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves perjuicios para la empresa.

La mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, englobados dentro de lo que se conoce como sistemas de información.

Estos sistemas de información están sujetos a riesgos y amenazas que pueden generarse desde dentro de la propia organización o desde el exterior.

Existen riesgos físicos como incendios, inundaciones, terremotos o vandalismo que pueden afectar la disponibilidad de nuestra información y recursos, haciendo inviable la continuidad de nuestro negocio si no estamos preparados para afrontarlos.

Por otra parte, se encuentran los riesgos lógicos relacionados con la propia tecnología y, que como hemos dicho, aumentan día a día. Hackers, robos de identidad, spam, virus, robos de información y espionaje industrial, por nombrar algunos, pueden acabar con la confianza de nuestros clientes y nuestra imagen en el mercado.

Para proteger a nuestras organizaciones de todas estas amenazas es necesario conocerlas y afrontarlas de una manera adecuada. Para ello debemos establecer unos procedimientos adecuados e implementar controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia.

Un Sistema de Gestión de Seguridad de la Información, basado en la norma UNE-ISO/IEC 27001, es una herramienta o metodología sencilla y de bajo coste que cualquier PYME puede utilizar. La norma le permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de su organización.

La implantación y posterior certificación de estos sistemas supone la implicación de toda la empresa, empezando por la dirección sin cuyo compromiso es imposible su puesta en marcha.

La dirección de la empresa debe liderar todo el proceso, ya que es la que conoce los riesgos del negocio y las obligaciones con sus clientes y accionistas mejor que nadie. Además, es la única que puede introducir los cambios de mentalidad, de procedimientos y de tareas que requiere el sistema.

Pero ¿qué es lo que aporta a mi negocio la implantación y posterior certificación de un Sistema de Gestión de Seguridad de la Información? ¿Cuáles son los beneficios que voy a observar después de todo este proceso?

En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible por nuestra organización. De este modo, si se produce una incidencia, los daños se **minimizan** y la continuidad del negocio está asegurada.

En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización.

En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

Por último, pero no por ello menos importante, la certificación del Sistema de Gestión de Seguridad de la Información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndolas más fiables e incrementando su prestigio.

Un certificado mejora la imagen y confianza de nuestra empresa entre clientes, proveedores y socios que, poco a poco, exigen la certificación para abrir y compartir sus sistemas de información con cualquier PYME. La exigencia de este certificado es el modo de garantizar un equilibrio en las medidas de seguridad entre las partes.

CAPÍTULO 3 – Marco legal y jurídico de la Seguridad. Normativas de Seguridad.

El creciente uso de las nuevas tecnologías ha propiciado la creación de un marco legal y jurídico que protege a todas las partes interesadas en el uso de estas tecnologías y el intercambio y tratamiento de la información a través de ellas.

Cada día surgen nuevas formas de delito informático que pueden afectar a la seguridad de la información en nuestras empresas.

Por ello, cumplir con la legislación vigente en España es uno de los requisitos que debemos satisfacer para implantar y certificar un Sistema de Gestión de Seguridad de la Información. Su cumplimento nos protegerá de amenazas externas, nos permitirá respetar los derechos de nuestros clientes y proveedores y evitará infracciones involuntarias con sus respectivos costes.

Veamos cuál es la legislación española relacionada con seguridad de la información, recordando el amplio sentido del término información visto anteriormente.

Ley Orgánica 15/99 de Protección de Datos de Carácter Personal conocida por las siglas LOPD.

Esta Ley tiene por objeto proteger todos los datos de carácter personal, para que no sean utilizados de forma inadecuada, ni tratados o cedidos a terceros sin consentimiento del titular.

Para ello, se establecen obligaciones para toda persona física o jurídica que posea ficheros con datos personales.

Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico cuyas siglas son LSSI.

La finalidad de esta Ley es regular el funcionamiento de **prestadores** de servicios de la Sociedad de la Información, empresas que realizan comercio electrónico, y aquellas que hacen publicidad por vía electrónica, como correo electrónico o SMS.

Ley 32/2003, General de telecomunicaciones.

El objeto de la Ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.

Entre otros objetivos, esta Ley fomenta la competencia efectiva de los mercados de las

telecomunicaciones, promueve el desarrollo del sector y defiende los intereses de los ciudadanos.

Ley 59/2003 de Firma Electrónica.

Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica es un conjunto de datos asociados que sirve para identificar a una persona en transacciones electrónicas y permite conocer si el contenido del mensaje ha sido manipulado de alguna manera.

Real Decreto Legislativo 1/1996 Ley de Propiedad Intelectual.

Según esta Ley, la propiedad **intelectual de una obra literaria, artística o científica corresponde al autor por el** solo hecho de su creación. El autor tiene el derecho exclusivo a la explotación de la obra.

La Ley protege las creaciones originales expresadas en cualquier medio, incluidos programas de ordenador o bases de datos.

Ley 17/2001 de Propiedad Industrial

Para la protección de los signos distintivos de las organizaciones se concederán los derechos de propiedad industrial de marcas y nombres comerciales.

De acuerdo con esta Ley, el uso de un nombre comercial en redes telemáticas, en nombres de dominios, y en metadatos y palabras clave de páginas web, sin autorización previa por parte de su titular, habilita a éste a prohibirle su utilización.

Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos

Esta ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. Además, regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas.

Algunos sectores, como el agrario poseen legislación propia sobre Seguridad de la Información.

Otros, como la banca, disponen de una normativa internacional que contiene recomendaciones al respecto.

La legislación que acabamos de ver se ha desarrollado para proteger a todos los actores que utilizamos las nuevas tecnologías ante el aumento de delitos informáticos.

En un sentido amplio, delito informático es todo aquel que implique la utilización de cualquier medio de tecnología informática.
Tanto en Europa como en España, los principales delitos informáticos que la legislación recoge se engloban en cuatro grupos.

El primer grupo hace referencia a los delitos contra la intimidad, en el que se produce un tratamiento ilegal de los datos de carácter personal. Este es el caso de la venta de datos a terceros sin autorización previa del dueño de esos datos.

El segundo grupo hace alusión a delitos relativos al contenido, es decir a la difusión de contenidos ilegales en la Red. Por ejemplo, la difusión de pornografía infantil.

El tercer grupo se refiere a delitos económicos, relacionados con el acceso autorizado a sistemas informáticos para llevar a cabo fraude, sabotaje o falsificación. Un caso muy habitual es la suplantación de entidades bancarias.

Y el cuarto grupo hace mención a los delitos contra la propiedad intelectual vinculados con la protección de programas de ordenador, bases de datos y derechos de autor. Un ejemplo claro es la piratería informática.

CAPÍTULO 4 – Estándares de Gestión de la Seguridad de la Información.

La información necesaria para desarrollar la actividad de nuestro negocio se puede ver afectada por diferentes riesgos y amenazas.

Para poder estar preparados ante cualquier imprevisto y actuar con rapidez y eficacia, es necesario implantar un Sistema de Gestión de Seguridad de la Información.

Gracias a este sistema podremos analizar los posibles riesgos, establecer las medidas de seguridad necesarias y disponer de controles que nos permitan evaluar la eficacia de esas medidas.

De este modo, podremos anticiparnos a los posibles problemas y estar preparados en el caso de cualquier contingencia.

Para llevar a cabo todo el proceso de una manera más sencilla contamos con la familia de normas internacionales ISO/IEC 27000.

Estas normas han sido elaboradas conjuntamente por ISO, que es la Organización Internacional de Normalización, y por IEC, que es la Comisión Electrotécnica Internacional. Ambos están formados por los organismos de normalización más representativos de cada país.

ISO e IEC se encargan de elaborar normas internacionales que el mercado requiere y necesita. Estas normas pueden hacer referencia a productos como electrodomésticos, calzado, alimentación o juguetes.

También **pueden** hacer referencia a servicios como los prestados en residencias de la tercera edad, en hoteles o en transportes públicos de pasajeros.

En los últimos años ISO e IEC han trabajado mucho con normas relacionadas con las nuevas tecnologías como la telefonía móvil o la seguridad de la información.

Y por supuesto, han continuado elaborado normas de gestión como las conocidas ISO 9001 e ISO 14001.

Las normas son de carácter voluntario, nadie obliga o vigila su cumplimiento. Sin embargo, su uso por millones de empresas facilita el entendimiento entre países y organizaciones. Las normas también contribuyen a mejorar la seguridad y la calidad de los productos y servicios que utilizamos todos los días.

Pero volvamos a las normas que ahora nos interesan, las normas ISO/IEC 27000 creadas para facilitar la implantación de Sistemas de Gestión de Seguridad de la Información. Veamos las más importantes.

La primera norma, la ISO/IEC 27000, recoge los términos y definiciones empleados en el resto de normas de la serie. Con ello se evitan distintas interpretaciones sobre los conceptos que aparecen a lo largo de las mismas.

Además, incluye una visión general de la familia de normas en este área, una introducción a los Sistemas de Gestión de Seguridad de la Información y una descripción del ciclo de mejora continua.

La norma principal de la serie es la ISO/IEC 27001. Se puede aplicar a cualquier tipo de organización, independientemente de su tamaño y de su actividad.

La norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización.

En España, esta norma ha sido publicada como UNE-ISO/IEC 27001 y puede adquirirse a través de la página web de AENOR, el organismo español de normalización, en www.aenor.es. Si se prefiere la versión en inglés se puede acceder a ella a través de la página de ISO, www.iso.org.

Esta es la norma de esta serie con la que serán certificados los Sistemas de Gestión de Seguridad de la Información de las empresas que lo deseen.

La norma ISO/IEC 27002 es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Para ello describe 11 dominios, es decir áreas de actuación, 39 objetivos de control **o** aspectos a asegurar dentro de cada área, y 133 controles **o** mecanismos para asegurar los distintos objetivos de control.

La familia de normas ISO/IEC 27000 contiene otras normas destacables. Como por ejemplo, la norma sobre requisitos para la acreditación de las entidades de auditoría y certificación, es decir, de aquellas entidades que acudirán a tu empresa para certificar que el sistema está correctamente implantado.

También incluye una guía de auditoría y guías de implantación de la norma en sectores específicos como el de sanidad o telecomunicaciones.

En el futuro se continuarán desarrollando nuevas normas relacionadas con la seguridad de la información que completen las necesidades de las empresas.

CAPÍTULO 5 – Implantación de un SGSI.

La implantación de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la dirección.

Su diseño dependerá de los objetivos y necesidades de la empresa, así como de su estructura. Estos elementos son los que van a definir el alcance de la implantación del sistema, es decir, las áreas que van a verse involucradas en el cambio. En ocasiones, no es necesario un sistema que implique a toda la organización, puede ser que sea sólo necesario en un departamento, una sede en concreto o un área de negocio.

Para hacer más sencillo el proceso de implantación, es bueno contar con la ayuda de una empresa especializada que nos asesore durante todo el proceso, especialmente durante el primer año. INTECO dispone de un catálogo que recoge un listado de empresas que pueden ayudarte en ello.

El tiempo de implantación del sistema de gestión de seguridad de la información varía en función del tamaño de la empresa, el estado inicial de la seguridad de la información y los recursos destinados a ello, pero podríamos estimar que su duración es de entre seis meses y un año para evitar que quede obsoleto nada más acabarlo.

Antes de entrar en más detalle sobre cómo debe realizarse la implantación del sistema, hay algo muy importante que hay que tener siempre presente: la solución más sencilla de implantar y mantener suele ser la más acertada.

La empresa debe contar con una estructura organizativa así como de recursos necesarios, entre otras cosas, para llevar a cabo la implantación del SGSI.

La metodología que acabamos de mencionar para medir y evaluar los resultados, debe estar en continúa evolución. Precisamente esa es la base de cualquier Sistema de Gestión de Seguridad de la Información. Por ello, para su implantación utilizaremos el modelo PDCA, un modelo dividido en cuatro fases en el que finalizada la última y analizados sus resultados se vuelve a comenzar de nuevo la primera.

Las siglas PDCA corresponden en inglés a Plan, Do, Check, Act y han sido traducidas como Planificación, Ejecución, Seguimiento y Mejora.

La continúa evaluación de nuestro Sistema de Gestión de Seguridad de la Información debe estar documentada, para lo que utilizaremos los cuatro tipos distintos de documentación que representamos en esta estructura piramidal.

En su cúspide se encuentran las Políticas que sientan las bases de la seguridad. Indican las líneas generales para conseguir los objetivos de la organización sin entrar en detalles técnicos. Toda la organización debe conocer estas Políticas.

En un segundo nivel se sitúan los Procedimientos que desarrollan los objetivos marcados por las Políticas. En ellos aparecen detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. Los Procedimientos deben ser conocidos por aquellas personas que lo requieran para el desarrollo de sus funciones.

En el tercer escalón aparecen las Instrucciones que constituyen el desarrollo de los Procedimientos. En ellos se describen los comandos técnicos que se deben realizar para la ejecución de los Procedimientos.

En el último escalón, se hayan los Registros que evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos. Entre estos Registros se incluyen indicadores y métricas de seguridad que permitan evaluar la consecuencia de los objetivos de seguridad establecidos.

La primera fase del Modelo PDCA para la implantación del sistema es la fase de Planificación.

Durante esta fase se realiza un estudio de la situación de la organización desde el punto de vista de la seguridad, para estimar las medidas que se van a implantar en función de las necesidades detectadas.

No toda la información de la que disponemos tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesaria una Gestión de dichos riesgos para reducirlos en la medida de lo posible.

Con el resultado obtenido en el Análisis y la Gestión de Riesgos estableceremos unos controles adecuados que nos permitan minimizar los riesgos.

En la fase de Ejecución del Modelo PDCA se lleva a cabo la implantación de los controles de seguridad seleccionados en la fase anterior. Estos controles se refieren a los controles más técnicos, así como a la documentación necesaria.

Esta fase también requiere un tiempo de concienciación y formación para dar a conocer qué se está haciendo y por qué, al personal de la empresa.

La tercera fase de nuestro Modelo PDCA es la fase de Seguimiento. En ella se evalúa la eficacia y el éxito de los controles implantados. Por ello, es muy importante contar con registros e indicadores que provengan de estos controles.

El Modelo PDCA se completa con la fase de Mejora durante la que se llevarán a cabo las labores de mantenimiento del sistema. Si durante la fase anterior de Seguimiento se ha detectado algún punto débil, este es el momento de mejorarlo o corregirlo.

Para ello se cuenta con tres tipos de medidas: medidas correctoras, medidas preventivas y medidas de mejora.

Al finalizar las cuatros fases, se toman los resultados de la última y se comienza nuevamente la primera.

Si el objetivo de la implantación de este sistema era la certificación, el ciclo completo tendrá una duración de un año, coincidiendo con las realizaciones de las auditorias de certificación que se realizan cada año.

CAPÍTULO 6 – Definición de las Políticas, Organización, Alcance del Sistema de Gestión y Concienciación.

La implantación de un Sistema de Gestión de Seguridad de la Información comienza con su correcto diseño. Para ello deberemos definir cuatro aspectos fundamentales. Primero, el alcance del sistema. Segundo, la Política de Seguridad a seguir. Tercero, la organización de la seguridad. Y cuarto, los programas de concienciación y formación del personal.

El primer paso, consiste en definir el alcance del sistema. Este debe determinar las partes o procesos de la organización que van a ser incluidos dentro del mismo. En este momento, la empresa debe determinar cuáles son los procesos críticos para su organización decidiendo qué es lo que quiere proteger y por dónde debe empezar.

Dentro del alcance deben quedar definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del sistema.

Es importante que durante esta fase, se estimen los recursos económicos y de personal que se van a dedicar a implantar y mantener el sistema. De nada sirve que la organización realice un esfuerzo importante durante la implantación si después no es capaz de mantenerlo.

Tras la definición del alcance, el siguiente paso es establecer la Política de Seguridad. Su principal objetivo es recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente. Además, debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.

El documento debe delimitar qué se tiene que proteger, de quién y por qué. Debe explicar qué es lo que está permitido y qué no; determinar los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan; e identificar los riesgos a los que está sometida la organización.

Para que la Política de Seguridad sea un documento de utilidad en la organización y cumpla con lo establecido en la norma UNE-ISO/IEC 27001 debe cumplir con los siguientes requisitos.

- Debe de ser redactada de una manera accesible para todo el personal de la organización. Por lo tanto debe ser corta, precisa y de fácil comprensión.
- Debe ser aprobada por la dirección y publicitada por la misma.
- Debe ser de dominio público dentro de la organización, por lo que debe estar disponible para su consulta siempre que sea necesario.
- Debe ser la referencia para la resolución de conflictos y otras cuestiones relativas a la

seguridad de la organización.

- Debe definir responsabilidades teniendo en cuenta que éstas van asociadas a la autoridad dentro de la compañía. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- Debe indicar que lo que se protege en la organización incluye tanto al personal como a la información, así como su reputación y continuidad.
- Debe ser personalizada totalmente para cada organización.
- Por último, debe señalar las normas y reglas que va a adoptar la organización y las medidas de seguridad que serán necesarias.

En lo que ser refiere al contenido, la Política de Seguridad debería incluir, al menos, los siguientes cinco apartados.

Uno. Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información.

Dos. Declaración por parte de la Dirección apoyando los objetivos y principios de la seguridad de la información.

Tres. Breve explicación de las políticas

Cuatro. Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca a personas concretas dentro de la organización.

Cinco. Referencias a documentación que pueda sustentar la política.

La Política de Seguridad debe ser un documento completamente actualizado, por lo que debe ser revisado y modificado anualmente. Además, existen otros tres casos en los que es imprescindible su revisión y actualización. El primero, después de grandes incidentes de seguridad. El segundo, después de una auditoría del sistema sin éxito. Y el tercero, frente a cambios que afectan a la estructura de la organización.

La organización de la seguridad es el tercer aspecto a desarrollar durante el diseño del Sistema de Gestión de Seguridad de la Información. En este momento, se realiza la revisión de los aspectos organizativos de la entidad y la asignación de nuevas responsabilidades.

Entre estas nuevas responsabilidades hay tres que tienen gran importancia.

El responsable de seguridad, que es la persona que se va a encargar de coordinar todas las actuaciones en materia de seguridad dentro de la empresa.

El Comité de Dirección que estará formado por los directivos de la empresa y que tendrá las máximas responsabilidades y aprobará las decisiones de alto nivel relativas al sistema.

Y por último, el Comité de Gestión, que controlará y gestionará las acciones de la implantación del sistema colaborando muy estrechamente con el responsable de seguridad de la entidad. Este comité tendrá potestad para asumir decisiones de seguridad y estará formado por personal de los diferentes departamentos involucrados en la implantación del sistema.

Al plantear la nueva organización de la seguridad hay que tener en cuenta la relación que se mantiene con terceras partes que pueden acceder a la información en algún momento, identificando posibles riesgos y tomando medidas al respecto. Por poner un ejemplo en el caso de los equipos de limpieza en una oficina, que suelen tener acceso a todos los despachos, se les podría requerir la firma de acuerdos de confidencialidad.

La última fase en el diseño del Sistema de Gestión de Seguridad de la Información consiste en la concienciación y formación del personal con el fin de crear en la empresa una cultura de seguridad.

La concienciación y la divulgación consiguen que el personal conozca qué actuaciones se están llevando a cabo y por qué se están realizando. Con ello se concede transparencia al proceso y se involucra al personal.

Por su parte, la formación logra que el personal desarrolle las nuevas actividades de acuerdo a la normativa y a los términos establecidos.

CAPÍTULO 7 – Los activos de la Seguridad de la Información.

Las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio. Este tipo de información imprescindible para las empresas es lo que se ha denominado activo de Seguridad de la Información. Su protección es el objetivo de todo Sistema de Gestión de Seguridad de la Información.

Los activos pueden dividirse en diferentes grupos según su naturaleza. Si seguimos la metodología de Magerit para agrupar activos, la utilizada en la Administración, estos son los tipos que encontramos.

En el primer tipo están los servicios, es decir, los procesos de negocio de la organización que ofrece la organización al exterior o que ofrece con carácter interno, como es el caso de la gestión de nóminas.

En el segundo grupo se encuentran los datos e información que se manipula dentro de la organización. Suelen ser el núcleo del sistema, mientras que el resto de activos suelen darle soporte de almacenamiento, manipulación, etcétera.

El tercer tipo está formado por las aplicaciones de software.

En el cuarto grupo están los equipos informáticos.

El quinto grupo lo forma el personal. Este es el activo principal. Incluye personal interno, subcontratado, de los clientes, etcétera.

En el sexto lugar están las redes de comunicaciones que dan soporte a la organización para el movimiento de la información. Pueden ser redes propias o subcontratadas a terceros.

El grupo séptimo lo configuran los soportes de información. Los soportes físicos que permiten el almacenamiento de la información durante un largo período de tiempo.

En el octavo grupo está el equipamiento auxiliar que da soporte a los sistemas de información y que son activos que no se han incluido en ninguno de los otros grupos. Por ejemplo, los equipos de destrucción de documentación o los equipos de climatización.

Y el último lugar se refiere a las instalaciones donde se alojan los sistemas de información, como oficinas, edificios o vehículos.

Junto a estos activos, hay que tener en cuenta aquellos intangibles como la imagen y la reputación de una empresa.

Para proteger los activos de información es necesario conocerlos e identificar cuáles son dentro de la organización. Para ello elaboraremos un inventario que los identifique y clasifique. Cada activo del inventario debe incluir, al menos, su descripción, localización y propietario.

El propietario del activo debe ser quien defina el grado de seguridad que requiere su activo.
El propietario no tiene, necesariamente, que ser quien va a gestionar el activo o ser su usuario. Por ejemplo, una base de datos de clientes puede pertenecer al Director Comercial de una empresa, su gestión puede estar encargada al área de sistemas y sus usuarios pueden ser los comerciales.

Una vez identificados todos los activos hay que realizar un análisis de las dependencias existentes entre ellos. Para establecer esas dependencias se pueden hacer preguntas del tipo ¿quién depende de quién? o ¿si hay un fallo en el activo X qué otros activos se van a ver perjudicados o involucrados?

El resultado de dicho análisis será un árbol de dependencias de activos en el que se podrá ver la relación existente entre todos los activos de una organización desde los de más alto nivel hasta llegar a los de nivel más bajo.

No todos los activos tienen la misma importancia para la organización, ni generan los mismos problemas sin son atacados. Por ello es necesario realizar una valoración de los activos en función de la relevancia que tengan para el negocio y del impacto que una incidencia sobre el mismo pueda causar a la entidad.

Podemos realizar una valoración cuantitativa, en la que se estima el valor económico del activo, o cualitativa.

La valoración cualitativa se establece de acuerdo a una escala, por ejemplo del 0 al 10 o con valores del tipo: bajo, medio y alto. En este tipo de valoración es muy importante que exista un criterio homogéneo de valoración que permita comparar entre activos. El criterio que se suele utilizar está basado en las características principales de la información: integridad, confidencialidad y disponibilidad.

Por ejemplo, si consideramos una base de datos de clientes como un activo de la organización, su valoración tiene que hacerse de acuerdo a estos tres parámetros principales. Para eso se debe responder a preguntas como ¿qué impacto tendría para el negocio que alguien tuviese acceso a la base de datos de clientes y modificase los datos de los mismos?

Aunque existen multitud de formas de valoración de los activos, la entrevista y la encuesta son los más utilizados. En ambos casos, se debe seleccionar un grupo significativo de personas entre el personal de la empresa. Estas personas deben representar a todas las áreas del alcance del Sistema de Gestión de la Seguridad de la Información, así como tener roles diferentes.

CAPÍTULO 8 – Análisis y Valoración de los Riesgos. Metodologías.

Antes de entrar de lleno en el análisis y valoración de los riesgos a los que deben hacer frente nuestros negocios, es importante entender algunos conceptos básicos tales como, riesgos, amenazas y vulnerabilidades, que nos van a facilitar el llevar a cabo un análisis y valoración adecuados.

La primera definición, como no puede ser de otra forma, se refiere a los riesgos. Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente.

Las amenazas son los eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos.

Las vulnerabilidades son las debilidades que tienen los activos o grupos de activos que pueden ser aprovechadas por una amenaza.

- El **impacto** es la consecuencia de la materialización de una amenaza sobre un activo.
- El **riesgo intrínseco** es la posibilidad de que se produzca un impacto determinado en un activo o en un grupo de activos.
- Las **salvaguardas** son las prácticas, procedimientos o mecanismos que reducen el riesgo. Estas pueden actuar disminuyendo el impacto o la probabilidad.
- Por último, tenemos la definición de **riesgo residual** que es el riesgo que queda tras la aplicación de salvaguardas. Por muy bien que protejamos nuestros activos, es imposible eliminar el riesgo al 100% por lo que siempre quedará un riesgo residual en el sistema que la organización deberá asumir y vigilar.

Conocer todos estos términos facilita la comprensión del tema que nos ocupa, el análisis de riesgos. Podríamos decir que este proceso consiste en identificar los riesgos de seguridad en nuestra empresa, determinar su magnitud e identificar las áreas que requieren implantar salvaguardas.

Gracias al análisis de riesgos conoceremos el impacto económico de un fallo de seguridad y la probabilidad realista de que ocurra ese fallo.

El análisis de riesgos tiene que cubrir las necesidades de seguridad de la organización teniendo siempre en cuenta los recursos económicos y humanos con los que ésta cuenta. La inversión en seguridad tiene que ser proporcional al riesgo.

Por ejemplo, imaginemos que una empresa tiene un servidor que contiene información definida como de valor bajo. Para acceder al despacho en el que se encuentra el servidor hay que acceder a través de un lector de retina, posteriormente para acceder al servidor hay que utilizar un lector de huella digital. Resulta evidente que las medidas adoptadas por la empresa son desproporcionadas teniendo en cuenta el valor de la información que contiene.

El análisis de riesgos aporta objetividad a los criterios en los que se apoya la seguridad ya que se centra en proteger los activos más críticos y permite a la organización gestionar los riesgos por sí misma. Además, apoya la toma de decisiones basándose en los riesgos propios.

Para evitar la subjetividad durante la realización del análisis es bueno contar con la colaboración de diversas áreas de la organización y no únicamente con el área propietaria del activo, ya que se evitará en gran medida la subjetividad que pueda tener el responsable de dicho activo.

Los análisis de riesgos deben utilizar unos criterios definidos claramente que se puedan reproducir en ocasiones sucesivas. De esta manera se puede ir comparando el nivel de riesgo en una organización a medida que se va mejorando el Sistema de Gestión de Seguridad de la Información.

El análisis de riesgos se basa en el inventario de activos que hemos realizado con anterioridad. Si nuestro inventario es muy extenso podemos decidir realizar el análisis de riesgos sólo de los activos más críticos.

A continuación, se identificarán las amenazas que pueden afectar a estos activos. Se realiza una valoración en función del impacto que la amenaza puede causarle en el caso de que se materialice.

Seguidamente, analizaremos las vulnerabilidades de los activos identificados y se realizará una valoración de las mismas. Si un activo está expuesto a una amenaza pero no tiene una vulnerabilidad que le permita manifestarse, el riesgo es menor que si existe la vulnerabilidad.

Una vez analizados los activos, las amenazas y las vulnerabilidades que pueden afectar a nuestros activos, se debe realizar un análisis de las salvaguardas o medidas de seguridad ya implantadas en la

organización.

Con todos estos datos podremos realizar el estudio del riesgo y el impacto de todas estas variables sobre los diferentes activos. Esto nos permitirá obtener los resultados del análisis de riesgos que definen a qué nivel de riesgo está expuesta la organización y tomar medidas al respecto.

El proceso del Análisis de Riesgos debe estar perfectamente documentado para poder justificar las acciones que se van a desarrollar y conseguir el nivel de seguridad que la organización quiere alcanzar.

Existen multitud de metodologías que nos pueden facilitar la realización de un análisis de riesgos. Estas metodologías nos indican los pasos a seguir para su correcta ejecución, ya que, como hemos visto, suelen ser muy complejos y tienen multitud de variables.

Utilizar una herramienta para llevar a cabo el análisis de riesgos facilita su elaboración y permite realizar las labores de manera más sistemática. Esto facilita que la información resultante sea reutilizable y comparable con resultados de sucesivos análisis.

Algunas de estas metodologías son: Magerit, la metodología detallada en la norma ISO/IEC 27005, OCTAVE, NIST SP 800 -30, etcétera.

CAPÍTULO 9 – Gestión y Tratamiento de los Riesgos. Selección de los Controles.

Tras haber determinado los riesgos existentes en nuestra organización debemos tomar las medidas adecuadas para hacer frente a los mismos. La gestión de riesgos es el proceso por el cual se controlan, minimizan o eliminan los riesgos que afecten a los activos de información de la organización.

Disponemos de varias opciones para afrontar estos riesgos:

En primer lugar, podemos eliminar el riesgo. Esto se consigue eliminando los activos a los que este riesgo está asociado. Se trata de una elección generalmente costosa y drástica por lo que suelen buscarse medidas alternativas.

La segunda opción consiste en transferir el riesgo. Para ello se valorará la subcontratación del servicio externamente o la contratación de un seguro que cubra los gastos en el caso de que ocurra una incidencia.

Hay casos en los que el valor del activo y el tipo de riesgo asociado al mismo, no hacen viable la subcontratación, como puede ser el caso de un activo altamente confidencial.

Cuando se piense en la contratación de un seguro, hay que asegurarse de que el valor del activo es superior al del propio seguro.

La tercera alternativa para hacer frente a un riesgo es asumirlo. Ello implica que no se van a tomar medidas de protección contra ese riesgo. La decisión ha de ser tomada y firmada por la dirección de la empresa y sólo es viable en el caso de que la organización controle el riesgo y vigile que no aumenta.

La última opción es mitigar el riesgo. Para ello la empresa debe implantar una serie de medidas que actúen de salvaguarda para los activos. Todas las medidas implantadas han de ser documentadas y gestionadas por la organización.

Una vez decididas las medidas que se aplicarán a los riesgos identificados, se realizará un nuevo análisis. El análisis resultante expondrá el Riesgo Residual de la organización. Es decir, el nivel de riesgo aceptable por la organización bajo el cual estarán todos los riesgos de la organización.

La norma ISO/IEC 27002 es una guía de buenas prácticas que ofrece una exhaustiva guía sobre los controles a implantar en nuestra organización y que debemos seguir si queremos certificar el Sistema de Gestión de Seguridad de la Información de nuestra organización con la norma UNE-ISO/IEC 27001.

La norma ISO/IEC 27002 contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Los dominios son áreas funcionales de seguridad. Por ejemplo, el dominio número 2 se refiere a los "aspectos organizativos de la seguridad de la información".

Para cada uno de estos dominios se definen una serie de objetivos que reflejan lo que se intenta conseguir a través de la implantación de cada uno de los dominios. En el dominio que hemos puesto como ejemplo anteriormente, existen dos objetivos. El primero está relacionado con la organización interna y dice cómo gestionar la seguridad dentro de la organización. El segundo está relacionado con la organización de terceros e indica cómo gestionar la seguridad de la organización y dispositivos manejados por terceros.

Los 133 controles correspondientes a los 39 objetivos son un conjunto de acciones, documentos, procedimientos y medidas técnicas a adoptar para el cumplimiento de los diversos objetivos. Siguiendo con el caso anterior, del objetivo de la organización interna se desprenden varios controles entre los que se encuentra la firma de acuerdos de confidencialidad.

Los controles son medidas de seguridad orientadas a mitigar los riesgos encontrados en el análisis de riesgos de manera que se encuentren por debajo del riesgo asumido por la organización.

Existen dos tipos de controles que se complementan: técnicos y organizativos.

Entre los controles técnicos se pueden encontrar, por ejemplo, la implantación de un antivirus o un cortafuegos. Estos controles tienen que quedar perfectamente documentados a través de procedimientos.

Los controles organizativos, por su parte, pueden quedar documentados a través de procedimientos, normativas o políticas de seguridad.

Los controles seleccionados por la organización serán recogidos en un documento llamado SOA, según las siglas en inglés de Statement of Applicability, y traducido como Declaración de Aplicabilidad.

El SOA recoge qué controles aplican en la organización y cuáles no.

Para aquellos controles que sí aplican se deben incluir los objetivos del control, la descripción, la razón para su selección/aplicación y la referencia al documento en el que se desarrolla su implantación.

Para aquellos controles no seleccionados, porque se considera que no aplican, se debe indicar la razón de su exclusión de manera detallada. Este punto es muy importante, ya que en la fase de certificación del sistema será uno de los documentos a revisar por los auditores. El documento debe mostrar que los controles no elegidos no se han escogido al azar o sin una razón de peso.

En el momento de seleccionar un control debemos tener en consideración las siguientes cuestiones:

- El coste del control frente al coste del impacto que supondría que el activo a proteger sufriera un incidente y el valor de dicho activo.
- La necesidad de disponibilidad del control.
- Qué controles ya existen.
- Qué supondría su implantación y mantenimiento, tanto en recursos económicos como en humanos.

Tras decidir qué controles son válidos para la organización se procederá a su implantación. Esta fase es una de las que requiere más tiempo y recursos de toda la empresa.

Para la implantación de los controles y las salvaguardas más técnicas se necesitará la colaboración de aquel personal que realiza estas labores técnicas. Mientras que para los controles organizativos será la dirección quien tenga que tomar decisiones, además de formar y concienciar a toda la entidad.

No es necesario el desarrollo de un procedimiento o documento por cada uno de los controles escogidos, sino que es más aconsejable agrupar diferentes controles para hacer más utilizable el sistema. Hemos de recordar que la solución más sencilla suele ser la más eficaz ya que es más fácil de implantar y de mantener.

Los controles implantados deberán ser revisados con regularidad para ver que su funcionamiento es el esperado. Está verificación tiene que ser realizada por el propietario del activo periódicamente en función de la criticidad y el valor del mismo.

A la vez, se han de establecer otro tipo de verificaciones por parte de la empresa a través de auditorías internas o externas.

Para verificar el correcto funcionamiento de un control implantado es muy importante haber establecido previamente una serie de objetivos e indicadores que nos permitan la medición de dicho funcionamiento.

CAPÍTULO 10 – Seguimiento, Monitorización y Registro de las Operaciones del Sistema.

El Sistema de Gestión de Seguridad de la Información debe ser revisado periódicamente para asegurar que se cumplan los objetivos marcados por la organización.

Para realizar este seguimiento es necesario establecer una serie de indicadores que nos permitan determinar el estado del sistema. El análisis de indicadores requiere que cada uno de los controles implantados esté asociado a una serie de registros que recopilen la información necesaria para el estudio del control.

Por ejemplo. Disponemos de un indicador cuyo objetivo es que el número de incidencias graves de seguridad no sea superior a una al año. Para poder medir el número de incidentes de este tipo, se crea un registro en el que se recojan las incidencias en el sistema y su nivel de gravedad. La revisión de estos registros permite observar si el sistema está funcionando tal y como se determinó en los objetivos.

El sistema contiene multitud de entradas y salidas que deben ser revisadas, alguna de ellas por la dirección. En concreto la dirección de la organización debe revisar los siguientes documentos:

- El informe de las auditorías internas que recoge el estado del sistema y de las incidencias detectadas.
- Los informes que el comité de gestión dirige al comité de dirección. Estos documentos son una fuente muy valiosa para el seguimiento del proyecto, ya que reflejan el estado del sistema y los puntos que requieren la supervisión de la dirección.
- El informe sobre las acciones realizadas por parte de los diferentes actores involucrados en el sistema.
- El resumen sobre el estado de las incidencias reportadas y la solución a las mismas.
- La revisión de los objetivos propuestos en cada una de las fases así como el grado de cumplimiento de los mismos.
- Y el resumen sobre los cambios sufridos en la organización.

Tras la revisión del Sistema de Gestión de Seguridad de la Información por parte de la dirección, se deberán ejecutar una serie de acciones dentro de la organización:

- En primer lugar, hay que decidir si es necesario realizar mejoras dentro del sistema, cuáles se van a llevar a cabo y su repercusión económica y laboral dentro de la organización.
- En segundo lugar, se tendrá que actualizar la evaluación y la gestión de riesgos. En el caso de que se hayan observado cambios significativos en la organización, es necesario realizar un nuevo Análisis de Riesgos y un plan de tratamiento de los mismos.
- Por último, hay que realizar una actualización de los procedimientos y controles si estos han dejado de ser útiles o están obsoletos.

Además de la revisión del sistema que realiza la dirección, es necesario llevar a cabo una revisión anual denominada auditoría interna. Esta auditoría puede ser realizada por personal de la propia entidad.

Durante las auditorías internas se realiza un listado de todos los controles a revisar y todos los aspectos del sistema que necesitan ser analizados. Con este listado el auditor realizará una revisión del sistema e indicará aquellos aspectos de mejora que se han detectado, así como la prioridad o gravedad de cada uno de ellos.

El auditor del sistema no debe haber participado en la implantación del mismo. Suele ser habitual que dentro de una empresa, unos departamentos auditen a otros como medida para mantener la objetividad y la independencia entre la implantación y la auditoría.

Debe realizarse una revisión completa del sistema una vez al año. Para ello se pueden planificar varias auditorías internas durante el año e ir revisando el sistema por partes. De este modo, sólo una parte de la organización estará pendiente de la auditoría, mientras que el resto puede continuar con su trabajo diario sin ninguna alteración.

Al finalizar la auditoria interna es necesario llevar a cabo dos tipos de acciones, unas para subsanar las incidencias encontradas y otras para mejorar el sistema. Estas acciones se realizan dentro de la última fase del modelo PDCA, vista con anterioridad, la Fase de Mejora.

Las acciones correctivas resuelven un problema observado durante las auditorías. Estas acciones pueden ir desde la actualización de un documento hasta el cambio de una infraestructura de red o de un responsable de un activo. Las acciones correctivas deben ser realizadas tan pronto como sean detectadas las incidencias.

Por su parte, las acciones preventivas no están asociadas a ningún problema encontrado en la auditoría aunque pueden responder a algún comentario realizado por el auditor sobre una posible mejora o alguna resolución tomada por la dirección de la empresa para mejorar el sistema.

Las acciones preventivas se deben implantar poco a poco para conseguir que el sistema sea cada vez más robusto. El sistema debe ir mejorando en cada ciclo PDCA.

El Sistema de Gestión de Seguridad de la Información contiene gran cantidad de controles e indicadores. Para facilitar la visión general de todos estos indicadores podemos utilizar un Cuadro de Mandos. Esta herramienta, además, ofrece una visión del estado de seguridad de la compañía y la definición de umbrales de alerta para los indicadores.

CAPÍTULO 11 – Gestión de la Continuidad del Negocio.

El negocio de una empresa depende de la información y los sistemas que la soportan. Por ello, hay que estar prevenidos ante la multitud de amenazas que pueden afectar a nuestra información.

Cuando una organización implanta la norma UNE-ISO/IEC 27001 lo que quiere conseguir es reducir sus riesgos y evitar posibles incidentes de seguridad. Sin embargo, hay que tener presente que existen situaciones que son imposibles de evitar, ya que no es posible proteger al 100% los activos de información, por eso las empresas tienen que planificarse con el fin de evitar que las actividades de su entidad queden interrumpidas.

Estos son algunos de los ejemplos que hemos encontrado en la prensa sobre los riesgos en materia de seguridad de la información.

- Las fallas eléctricas causan el 90% de los incendios. Los problemas más comunes por los que se produce este tipo de siniestros son: la utilización de materiales no adecuados, un cálculo erróneo del sistema o contratar electricistas sin formación técnica.
- El 43% de las empresas estadounidenses que sufren un desastre, sin contar con un Plan de Continuidad del Negocio, no se recuperan. El 51% sobrevive pero tarda un promedio de dos años en reinsertarse en el mercado y solo el 6% mantiene su negocio a largo plazo.
- El 30% de las copias de seguridad y el 50% de las restauraciones fallan, según un informe de Enterprise Strategy Group. Durante este estudio muchos departamentos de Tecnología de la Información reconocían no estar seguros de ser capaces de recuperar los datos críticos del negocio y si podrían hacerlo en un tiempo razonable.

Para evitar estas y otras situaciones es necesario disponer de un Plan de Continuidad del Negocio. Este plan es la respuesta prevista por la empresa ante aquellas situaciones de riesgo que le pueden afectan de forma crítica.

No importa el tamaño de la empresa o el coste de las medidas de seguridad implantadas, toda organización necesita un Plan de Continuidad del Negocio, ya que tarde o temprano se encontrará con una incidencia de seguridad.

En líneas generales podemos decir, que estos planes tienen como objetivo impedir que la actividad de la empresa se interrumpa y, si no puede evitarse, que el tiempo de inactividad sea el mínimo posible.

Pero además, tienen que intentar lo siguiente:

- Mantener el nivel de servicio en los límites definidos por la compañía y que han sido asumidos por la misma.
- Establecer un periodo de recuperación mínimo para garantizar la continuidad del negocio. Algunas compañías pueden parar su actividad, debido a una incidencia, durante una semana pero otras no pueden superar unas horas.
- Recuperar la situación inicial de los servicios y procesos. La recuperación no tiene que ser inmediata y toda al mismo tiempo, ya que puede que existan procesos más críticos que necesiten recuperarse antes.
- Analizar el resultado de la aplicación del plan y los motivos del fallo para optimizar las acciones a futuro. Es decir, aprender de las incidencias para mejorar en la respuesta.

Cuando desarrollemos nuestro Plan de Continuidad del Negocio tenemos que tener en cuenta que debe contener los siguientes apartados:

- Establecimiento y definición de las situaciones críticas. Para ello se han de identificar, entre los riesgos analizados, aquellos que no podrán ser evitados a través de las diversas medidas implantadas.
- Establecimiento de un Comité de Emergencia que será el encargado de gestionar la situación de crisis ante una incidencia. Es el responsable de organizar al resto del personal y de que la empresa pueda recuperarse de un incidente.
- Definición de las diversas situaciones posibles, elaborando procedimientos para cada una de las incidencias que se podrían dar en una organización. Estos procedimientos recogerán:
  - En primer lugar, la situación que provocará una incidencia determinada. Al producirse esta situación se deben comenzar las acciones para evitar que el daño vaya a más y para comenzar la recuperación.
  - En segundo lugar, todas las acciones y las secuencias que deben llevarse a cabo ante un incidente de seguridad. Las prisas y las situaciones de estrés, provocadas por este tipo de incidencias, pueden hacer que no se lleven a cabo las acciones como se deberían. Por ello, es importante tener por escrito todo el procedimiento detallado y éste, debe ser conocido por las personas implicadas.
  - Y por último, contener los registros que es necesario recoger durante la incidencia para su posterior análisis y realización de acciones de mejora.

El plan debe haber sido probado y mejorado antes de que haya que aplicarlo. De no ser así, puede ser

que en el momento de producirse el incidente el plan falle y no nos sirva para salir de la situación sino que la empeore.

Así mismo, el plan debe ser conocido por todo el personal involucrado directa e indirectamente. El grado de conocimiento del plan por parte de los diferentes actores dependerá de su involucración dentro del mismo.

Para desarrollar un Plan de Continuidad del Negocio es necesario seguir cuidadosamente las siguientes fases:

- Primera fase. Definición del proyecto, donde es necesario establecer los objetivos, el alcance y el peor de los escenarios.
- Segunda fase. Análisis de impacto en el negocio, conocido por sus siglas en inglés BIA (Business Impact Analysis). Debemos realizar un análisis de riesgos, evaluar el impacto del incidente tanto económico como de cualquier otro tipo, identificar los procesos y activos críticos, asignar el tiempo objetivo de recuperación y evaluar las coberturas de los seguros y contratos.
- Tercera fase. Selección de estrategias. Aquí hay que identificar los recursos disponibles, evaluar las salvaguardas y estimar si conviene más aportar una solución a nivel interno o a nivel externo.

  Con toda la información hay que valorar las ventajas y desventajas de cada una de las estrategias posibles y escoger la más conveniente para la organización.
- Cuarta fase. Desarrollo de planes en los que tenemos que implementar diferentes procedimientos para afrontar las diversas incidencias.
- Quinta fase. Pruebas y mantenimiento del plan de continuidad.

Es imprescindible probar el plan para garantizar que cuando haya que usarlo todo funcione como está previsto.

El plan debe ser probado periódicamente para identificar y corregir posibles deficiencias e incluir actualizaciones del sistema. Estas pruebas deben incluir, al menos, la restauración de las copias de seguridad, la coordinación del personal y departamentos involucrados, la verificación de la conectividad de los datos y del rendimiento de los sistemas alternativos, y la verificación del procedimiento para la notificación de las incidencias y la vuelta a la situación inicial de normalidad.

CAPÍTULO 12 – Proceso de Certificación.

Al finalizar la implantación del Sistema de Gestión de Seguridad de la Información tenemos la opción de certificarlo, es decir, obtener un documento a través de un tercero de confianza que verifica su correcta implantación.

Con ello certificamos la gestión del sistema pero no las medidas implantadas o la seguridad de la empresa. Lo que certifica es que la empresa gestiona adecuadamente la seguridad.

Las empresas certifican sus sistemas, entre otras razones, para mejorar su imagen, porque sus clientes lo demanda o porque creen que es bueno para su gestión interna.

Para poder certificarlo, nuestro Sistema de Gestión de Seguridad de la información tiene que estar basado en la norma UNE-ISO/IEC 27001. Además, debe estar implantado y funcionando y tienen que existir evidencias que lo demuestren. Así mismo, tiene que contar con recursos económicos y personal de la empresa para atender a las demandas de la entidad de certificación.

En el momento de contratar a una entidad de certificación, debemos asegurarnos de que cuenta con auditores cualificados para verificar la correcta implantación del sistema según la norma UNE-ISO/IEC 27001.

Además, deberemos comprobar que posee la adecuada acreditación que la reconoce como una entidad competente para la realización de esa actividad. La entidad de certificación debe estar acreditada para la norma en la que se desea realizar la certificación, asegurando así que cumple con los requisitos para realizar correctamente su trabajo.

La entidad de acreditación española es ENAC, aunque existen numerosas entidades de acreditación en todo el mundo. Las empresas certificadoras podrían estar acreditadas por una entidad que no fuese la española. En este caso sería necesario que la entidad de acreditación validase las actividades también en el territorio español, indicándolo específicamente en sus credenciales.

El proceso de certificación puede variar ligeramente dependiendo de la entidad de certificación que lleve a cabo el proceso, sin embargo hay una serie de etapas comunes para todas ellas:

- Comenzaremos gestionando la solicitud de certificación: La empresa debe solicitar una oferta a la entidad de certificación en la que se especificarán una serie de datos sobre la organización y

la implantación del SGSI, tales como el alcance, el número de empleados y los centros de trabajo dentro del alcance, etcétera. Con ello se calcula el precio y el número de días de duración de la auditoría así como el número de auditores que la llevarán a cabo.

- A continuación tiene lugar la auditoría documental, que es la primera fase de la auditoría: En ella se revisa la documentación generada durante la implantación del sistema y que incluirá, al menos, la política de seguridad, el alcance de la certificación, el análisis de riesgos, la selección de los controles de acuerdo con la declaración de aplicabilidad (SOA) y la revisión de la documentación de los controles seleccionados por la entidad de certificación.
- La segunda fase de la auditoría es la auditoría in-situ: Tiene lugar en la empresa, a la que se desplazan los auditores para verificar la documentación revisada en la fase anterior así como los registros del sistema. Durante esta fase los auditores confirman que la organización cumple con sus políticas y procedimientos, comprueban que el sistema desarrollado está conforme con las especificaciones de la norma y verifican que está logrando los objetivos que la organización se ha marcado.

Después de cada una de las fases de la auditoría la entidad de certificación emite un informe en el que se indican los resultados de la misma. En estos informes pueden aparecer los siguientes resultados:

- **Uno.** Todo correcto.
- **Dos.** Observaciones sobre el sistema que no tienen excesiva relevancia pero que deben ser tenidas en cuenta en la siguiente fase de la auditoría, bien para ser revisadas in-situ o bien para ser mejoradas en el siguiente ciclo de mejora.
- **Tres.** No conformidades menores. Estas son incidencias encontradas en la implantación subsanables mediante la presentación de un Plan de Acciones Correctivas en el que se identifica la incidencia y la manera de solucionarla.
- **Cuatro.** No conformidades mayores que deben ser subsanadas por la empresa. Sin su resolución y, en la mayor parte de los casos, la realización de una auditoría extraordinaria por parte de la entidad de certificación, no se obtendría el certificado ya que se trata de incumplimientos graves de la norma
  En caso de darse tras la auditoría documental es necesario su resolución antes de llevar a cabo la auditoría in-situ.

Una vez conseguido el certificado del sistema, éste tiene una validez de tres años, aunque está sujeto a revisiones anuales.

Durante el primer año se realiza la auditoría inicial. Posteriormente cada tres años se realiza una

auditoría de renovación. En los dos años posteriores tanto a la auditoría inicial como a las de renovación se realizarán auditorías de seguimiento.