Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID

ESCUELA DE INGENIERIAS INDUSTRIALES

Grado en Ingeniería en Organización Industrial

Cómo gestionar la seguridad de la información (según ISO 27001: 2013) en una PYME del sector de las tecnologías de la información y la comunicación

Autor:
Abad Peña, María Belén

Tutor:
Posada Calvo, Marta
Departamento: Organización de Empresas y CIM

Valladolid, Julio 2015

AGRADECIMIENTOS

El camino ha sido largo y difícil, pero hay dos personas a las que les debo todo, ellos fueron quienes tuvieron la certeza de que lo conseguiría, incluso cuando me faltaron las fuerzas. A mis padres, Pilar y Francisco, esto y todo que venga detrás, es por y para vosotros.

Gracias a Andrés por acompañarme siempre sin importar el tiempo ni la distancia.

Gracias a mi tutora, Marta, por el apoyar mi propuesta y sobre todo por sus consejos y su ayuda.

Gracias a toda mi familia y amigos por el apoyo a lo largo de estos años, en especial a Itos y Feli por todo lo que he aprendido de vuestra fortaleza, gracias por luchar y vencer, es un regalo para mí que podáis disfrutar este momento conmigo.

Y por último, a las personas que he perdido en este camino, pero que nunca dejan de estar conmigo, Tía Rosa, Alba. Gracias.

RESUMEN

Este proyecto es una guía para ayudar a pequeñas y medianas empresas (PYMES) a adquirir el conocimiento suficiente sobre la norma ISO/IEC 27001:2013 para poder optar a la certificación ISO de la misma. Para ello se comienza desarrollando los conceptos de información y de Sistema de gestión de seguridad de la información (SGSI), analizando por qué es necesario su implantación y cuáles son sus beneficios, también se analiza el sector IT mediante un análisis de las cinco fuerzas de Porter. A continuación se introduce la serie de normas 27001, y se explica en detalle la norma que nos interesa, la ISO/IEC 27001:2013 comparándola con su predecesora ISO/IEC 27001:2005. Por último se adjunta una documentación mínima propuesta cuyo fin es ayudar al lector a considerar todo lo que la norma expone que requiere quedar reflejado como información documentada.

PALABRAS CLAVE:

27001, Seguridad, Información, Calidad, Certificación, PYMES.

SUMMARY

This dissertation is a guide created to help small and medium enterprises to acquire enough knowledge about ISO/IEC 27001:2013 that allows them to get the ISO certification. To do so, it starts by developing the concepts of information and information security management system (ISMS), analyzing why it is necessary its implementation and which are its benefits, IT sector is also analyzed by using Porter's Five Forces. Then, the 27001 standards are introduced, and a detailed description of ISO/IEC 27001:2013 is given, comparing it to its predecessor ISO/IEC 27001:2005. Finally, a minimal suggested documentation is attached in order to cover every part of the standard that requires to be available as documented information.

PALABRAS CLAVE:
27001, Security, Information, Quality, Certification, SMEs.

ÍNDICES

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

OBJETIVO Y ANTECEDENTES

El objeto de este proyecto es proporcionar al pequeño y mediano empresario una metodología a seguir que le permita conseguir la certificación en la norma *UNE-ISO/IEC 27001:2014 "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos."*, sin la necesidad de recurrir a ninguna contratación externa.

ISO/IEC 27001 "Information technology. Security techniques. Information security management systems. Requirements." es un estándar para la seguridad de la información en el que se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información de acuerdo con el Ciclo de Deming: Planificar-Hacer-Comprobar- Actuar (ciclo PDCA).

En el año 2005 se publica la primera versión, cuya versión española es *UNE-ISO/IEC 27001:2007 "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos"* (AENOR 2007). La nueva *ISO 27001:2013*, y su respectiva traducción al español *UNE-ISO/IEC 27001:2014* introduce varios cambios (AENOR 2014).

La idea de este trabajo se genera tras cursar las prácticas curriculares del 22/julio/2013 al 13/septiembre/2013 en el departamento de calidad de una empresa mediana (200 empleados), cuya desempeño se basa en la oferta y gestión de servicios relacionados con las tecnologías de la información y que, por propuesta propia y/o sugerencia de los clientes, cuenta con las siguientes certificaciones:

- *ISO 9001:2008*, Sistema de gestión de la calidad
- *ISO 14001: 2004*, Sistema de Gestión Ambiental
- *ISO/IEC 27001:2005*, Seguridad de la información
- *ISO/IEC 20000-1:2011*, Tecnologías de la Información

Para el desarrollo de esta idea se requería formación adicional a la recibida en el Grado de Ingeniería en Organización Industrial sobre ciberseguridad (en concreto, conocimientos sobre la seguridad de la información y sus dominio), que la autora ha adquirido tras realizar el curso *Cybersecurity and Its Ten Domains* ofrecido por la *University System of Georgia*, realizado íntegramente por los profesores Dr. Humayun Zafar y Mr. Andy Green, especialistas en seguridad de la información. El curso se centra en conocimiento sobre el acceso a los materiales que se ocupan de la identificación y la gestión de

riesgos, el cumplimiento, la continuidad del negocio y recuperación de desastres, la criptografía, seguridad de desarrollo de software, control de acceso, seguridad de redes, arquitectura de seguridad, las operaciones de seguridad, y la seguridad física y ambiental.

RELEVANCIA DEL TEMA

La información en las entidades y su tratamiento, indistintamente de su tamaño, ha tomado una importancia creciente en la última década. Como consecuencia directa de la concienciación sobre la protección de datos, el número de certificaciones expedidas en los últimos años ha aumentado tanto en ámbito internacional como nacional.

Contemplando las cifras estadísticas en el ámbito internacional observamos una tendencia constante en el aumento de certificaciones en la norma *ISO/IEC 27001* desde año 2006 hasta el 2013 (ver Figura 1). Los últimos datos recogidos muestran que, a finales del año 2013 se alcanzaron un total de 22293 organizaciones certificadas en *ISO/IEC 27001:2005* en 105 países, registrándose un aumento del 14% sobre la cifra de 19557, el mismo dato del año 2012 en 103 países. Observamos que el rango anual de aumento varía, pero el hecho de que durante los años de declive económico no se produzca una disminución del número de certificaciones es muestra de su relevancia.

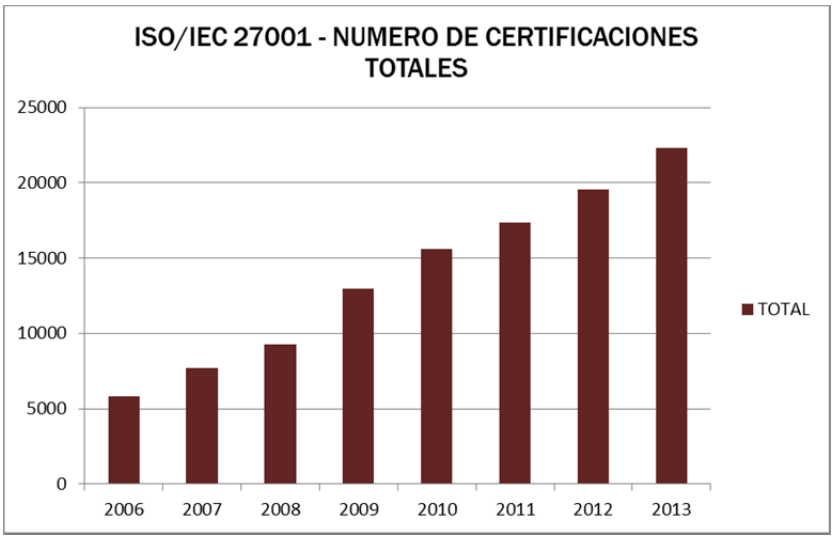

Figura 1: ISO/IEC 27001 Número de certificaciones desde 2006 hasta 2013.
Fuente: ISO.org .

En el caso de España, esta tendencia al aumento de certificaciones se mantiene, aunque de forma discontinua (ver Figura 2). Si bien el crecimiento en los primeros años ha sido mucho mayor (pasando de un total de 21 certificaciones en 2006 a 738 en 2009, en el 2010 y 2012), se contemplan dos tendencias de disminución de las certificaciones, repercusión de la aguda recesión económica.

Figura2: ISO/IEC 27001 Número de certificaciones en España desde 2006 hasta 2012.
Fuente: ISO.org.

Cabe destacar la excelente posición de España, que se encuentra en la lista de los 10 países donde se emitieron más certificaciones ISO/IEC 27001 en el año 2012 (ver Figura 3) y de los 10 países donde estas certificaciones más aumentaron (ver Figura 4).

Figura 3: Los 10 países con mayor número de certificaciones ISO/IEC 27001 en el 2012.
Fuente: ISO.org.

Figura 4: Los 10 países con mayor número de crecimiento en las certificaciones ISO/IEC 27001, año 2012. Fuente: ISO.org.

La norma *ISO/IEC* 27001 es aplicable a cualquier organización independientemente de su tamaño o sector, puesto que en todas encontramos volúmenes de información con los que hay que trabajar y sobre los que hay que garantizar cierta seguridad.

En cuanto al análisis por sectores industriales (ver Figura 5), en el año 2012 a nivel internacional, se impone sobre todos las tecnologías de la información (*IT - Information Technology*), puesto que la certificación es especialmente adecuada cuando la protección de la información es crítica como sucede en IT.

RELEVANCIA DEL TRABAJO

Habitualmente las grandes compañías cuentan con un consolidado departamento de calidad que les permite, siguiendo planes completos y precisos, obtener las certificaciones en calidad, medioambiente, Seguridad de la información, Tecnologías de la Información, etc.

En el caso de PYMES, el empresario es consciente de la necesidad de obtener ciertas certificaciones. Para ello, es habitual que se recurra a la contratación de una empresa externa especializada en ello.

Esta contratación externa, a la hora de plantearse obtener una certificación, es necesaria si no tiene ningún conocimiento previo ni experiencia, porque si

no, es complicado saber por dónde empezar. Este trabajo es una guía que permite conseguir la certificación en la norma *ISO/IEC 27001:2013*, sin la necesidad de recurrir a ninguna contratación externa, permitiéndole así al pequeño y mediano empresario prescindir de un gasto importante.

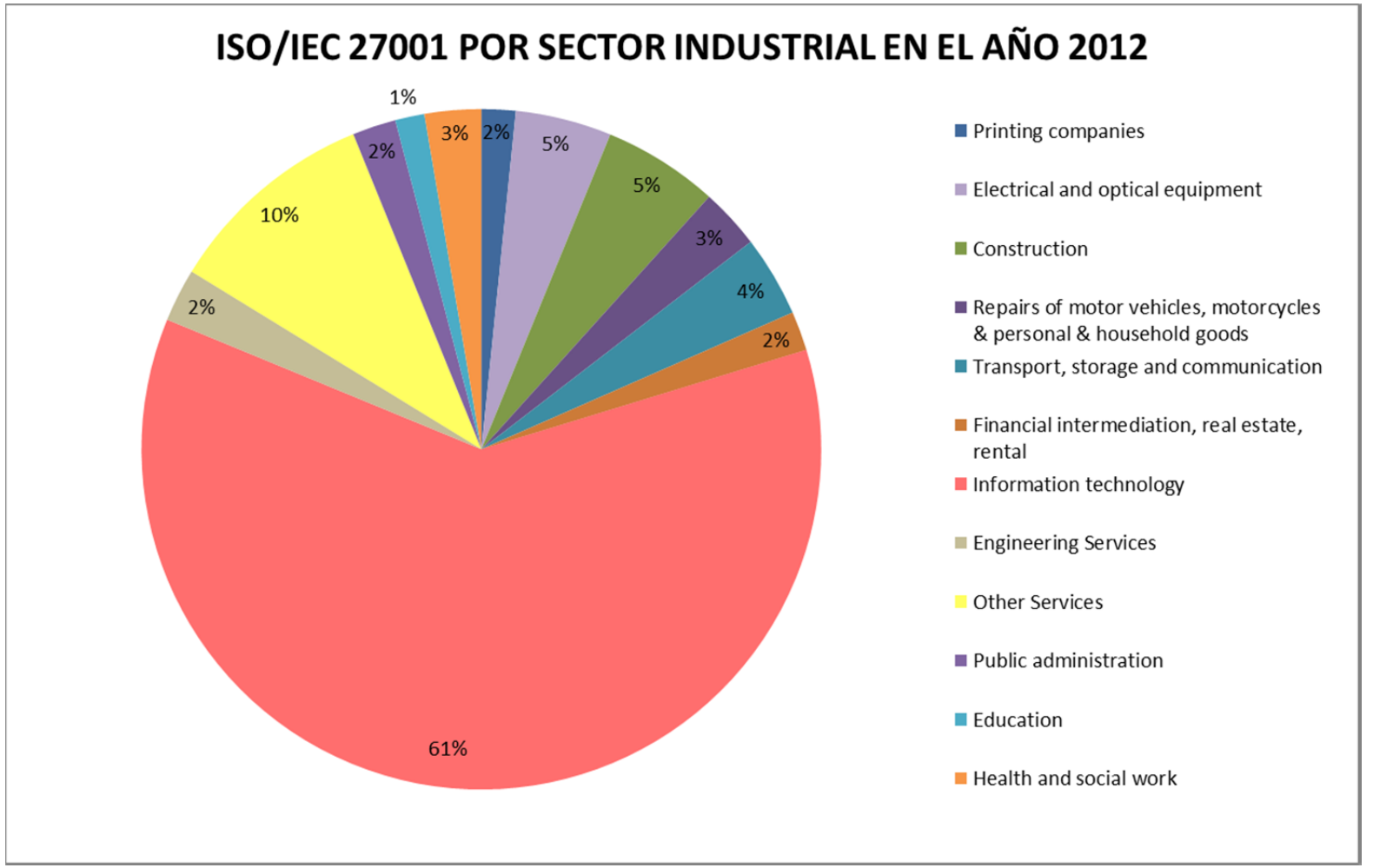

Figura 5: ISO/IEC 27001 Análisis por sectores de industriales de certificaciones a nivel mundial en el año 2012.Fuente: ISO.org

ESTRUCTURA

El presente trabajo se estructura 3 capítulos, además de la introducción, las conclusiones y la bibliografía.

El primer capítulo encontramos los conceptos clave para ir sumergiendo al lector en el concepto de "información" y en la necesidad que a día de hoy supone la creación y mantenimiento de un sistema de gestión de seguridad de la información (SGSI). Se desarrolla también un análisis completo, mediante fuerzas de portes, del sector en que más importancia toma el SGSI, las tecnologías de la información.

A continuación, en el segundo capítulo se introduce la *ISO/IEC 27001* de acuerdo con el Ciclo de Deming: Planificar-Hacer-Comprobar-Actuar y se define en detalle cada una de las cláusulas de la *ISO/IEC 27001:2013*, la norma objeto de este trabajo, así como una referencia a los cambios que se han realizado en la nueva versión de la norma para aquellos que estuviesen familiarizados con le versión del 2005.

En el tercer capítulo se propone una documentación que permita a la empresa cumplir con todos los puntos de la norma y que esto quede reflejado de forma clara y ordenada. En concreto, se desarrolla la documentación para:

- Planificar: política, acciones para tratar los riegos de seguridad, los objetivos de seguridad, competencias,
- Hacer: planificación y control operacional, apreciación de los riesgos de seguridad, tratamiento de los riesgos de seguridad
- Comprobar: Seguimiento y medición, auditoria interna, revisión por la dirección.

Para terminar, se incluyen las conclusiones finales de este estudio.

CAPÍTULO 1

LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1.1 INTRODUCCIÓN

1.1.1 INFORMACIÓN: DEFINICIÓN Y EVOLUCIÓN

Actualmente, el Diccionario de la Real Academia Española nos ofrece dos de las definiciones de información más significativas:

> "*Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada*."

> "*Conocimientos así comunicados o adquiridos*."

Linares y Patterson (1999) hacen un recorrido del papel de la información en la historia del hombre. Desde el comienzo de los tiempos el ser humano ha transmitido información, incluso antes de que se pudiese dejar por escrito, los conocimientos adquiridos se transmitieron de generación en generación mejorándose y ampliándose.

La aparición de la escritura permitió al fin que todo el conocimiento acumulado durante siglos quedase plasmado. A mediados del siglo XV los manuscritos dejaron paso a la imprenta, que no solo facilitó la tarea de los copistas sino que fue la herramienta necesaria a la hora de expandir la cultura y dar a conocer cualquier información alrededor del mundo.

Con el comienzo del siglo XX, inventos como la radio o la televisión cambiaron el concepto tradicional de tratamiento de la información. Pero la verdadera revolución estaba por llegar, con la aparición de las computadoras y de las primeras redes de comunicación entre las mismas el volumen de la información crece de forma exponencial. En la última década no dejan de aparecer conceptos asociados a esta constante incremento, como el de Sociedad de la información y del Conocimiento, que se refiere a la facilidad de acceso a la información y la capacidad creciente de almacenamiento y difusión de la misma, o el de Tecnologías de la información (TICS) cuya misión es ofrecer recursos y técnicas para el manejo de la misma (Linares y Patterson 1999).

1.1.2 VOLUMEN Y TRATAMIENTO DE LA INFORMACIÓN EN PYMES.

Las organizaciones son partes activas y fundamentales de nuestra sociedad, conocen la importancia de la información y son conscientes de que ésta siempre ha jugado un papel trascendental en beneficio de quien la poseía, no solo representa riqueza, si no la capacidad de generarla.

Para una pequeña o mediana empresa una buena gestión de la información es fundamental, puede marcar las posibilidades de éxito o fracaso de nuestro negocio. Es necesario saber manejar con la información de forma rigurosa, pero también se hace imprescindible el manejo de TICS que nos permitan optimizar este trabajo.

Actualmente la información es uno de los activos más valiosos de las organizaciones (Landoll 2011). Por ello, necesita contar con una serie de medios que garanticen su buen uso y la protejan de amenazas.

En la legislación española, la Ley de Protección de Datos (LOPD), que tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". Se aplicará tanto a los ficheros públicos como privados que contengan datos de carácter personal (San Martín 2004).

1.2 DEFINICIÓN DE UN SGSI

Un Sistema de Gestión de Seguridad de la Información va más allá de las exigencias de la legislación. Sin embargo, antes de avanzar en este ámbito es necesario proporcionar una definición adecuada de un sistema de gestión.

En la primera versión de la norma *ISO/IEC 27001:2005 se* define un Sistema de Gestión de Seguridad de la Información como "*la parte de sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos"* (AENOR 2007).

La implantación de este sistema supondrá un cambio radical para las organizaciones, se deja atrás la manera de operar que hasta ahora se había llevado a cabo, sustituyendo las medidas tomadas de forma intuitiva por sistemas de información con acceso ordenado. Esta implantación nos permitirá un mejor conocimiento de la organización y su funcionamiento, facilitando así el acceso a la información necesaria para determinar una estrategia específica para que la organización mejore sus datos.

1.3 ¿POR QUÉ ES NECESARIO UN SGSI?

Un sistema de seguridad de la información se convierte en necesario en el momento en que la disponibilidad, integridad y confidencialidad de la información de la organización se ve amenazado (Díaz *et al* 2008).

Actualmente todas las entidades poseen información privada y esta es considerada su mayor activo. La cantidad de amenazas a las que se ve sometida aumenta cada día y por tanto es evidente que la organización debe tomar el camino necesario para protegerse (Corletti 2007).

1.3.1 NATURALEZA DE AMENAZAS A LA INFORMACIÓN

Alberts y Dorofee (2003) definen una amenaza como la indicación de un potencial evento no deseado. Existe un amplio rango de amenazas, de muy diversas naturalezas ante las que la información es vulnerable, estas provienen tanto del exterior como del interior de la organización.

Durante el año 2012 el 83% de las organizaciones sufrieron un ataque a su seguridad y de estos, el 58% fue causado desde el interior (empleados, ex empleados, intermediarios) frente al 42% de los ataques externos (ver Figura 1.1).

Los ataques externos engloban amenazas naturales (inundaciones, tornados), amenazas a las instalaciones (fuegos, humedades) y amenazas tecnológicas tanto intencionadas como no intencionadas (virus informáticos, hacking, fallos de hardware). Las cantidades destinadas a tratar de evitar o solventar los daños causados por virus implican a veces sumas exageradas una buena estrategia puede consistir en, una vez identificadas las amenazas se debe considerar su posibilidad de ocurrencia, de esta forma se hará más sencilla la tarea de desarrollar un plan eficiente de seguridad (Alexander 2007).

Desde el interior de la organización la amenaza es igual de seria y es prácticamente imposible predecir qué tipo de ataque puede acontecer, cuando se producirá o cual será su gravedad. La encuesta publicada en mayo de 2013 en el blog especializado en tecnología Clearswift (www.clearswift.com) nos proporciona una información muy representativa en cuanto a las amenazas internas. Aunque solo considera organizaciones del Reino Unido, los resultados revelan que el 42% de las amenazas son de naturaleza externa frente al 58% de naturaleza interna y que los empleados son la causa del 33% de las amenazas.

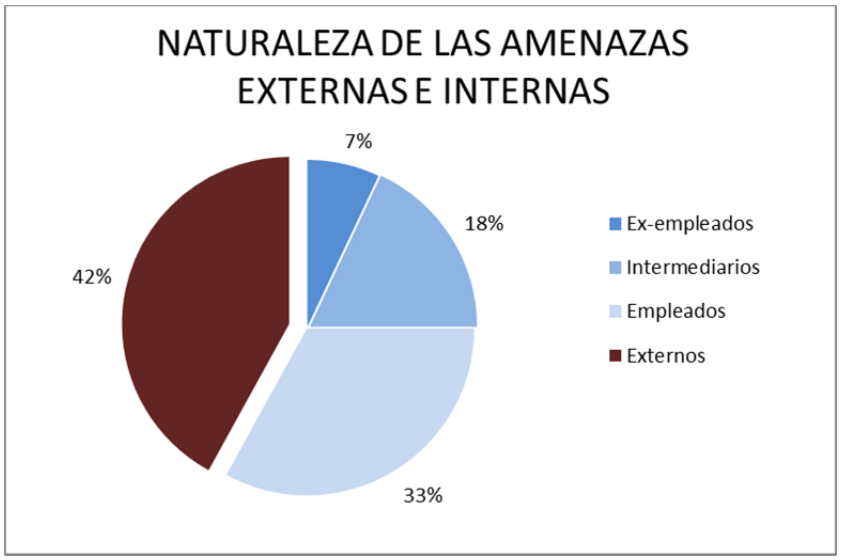

Figure 1.1: Gráfico de relación de los tipos de naturaleza de las amenazas.
Fuente: www.clearswift.com.

En la mayor parte de pequeñas y medianas organizaciones todavía no existe suficiente consciencia y comprensión a la hora de implantar medidas que combatan las amenazas a la seguridad de la información, especialmente aquellos que son cometidos por la mano del hombre. Es por esto que, en muchas ocasiones en las PYMES, la seguridad de la información es interpretada como una competencia exclusiva del departamento de Informática y Tecnología, pero eso no debe ser así, el éxito de un buen plan de seguridad empieza por el compromiso de la dirección y busca minimizar los riesgos implementando unas prácticas de sentido común en los empleados a la hora de manejar las herramientas. Además, es completamente necesario mantener una documentación elaborada sobre estas amenazas a la seguridad porque serán el pilar a la hora de considerar los riesgos a los que se expone la información de la organización.

1.3.1 METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Existen infinitas posibilidades a la hora de analizar y gestionar la seguridad de la información y los riesgos que su mantenimiento conlleva.

La entidad es libre de elegir si crear su propia metodología, con el esfuerzo y tiempo que esto supondría, o adoptar alguna de las ya existentes: MAGERIT, CRAMM, OCTAVE (ver Figura 1.2).

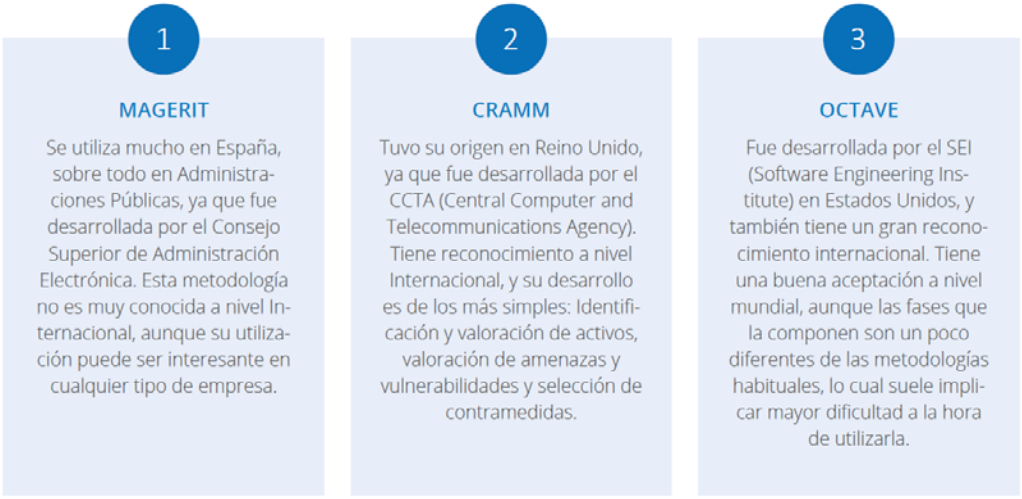

Figura 1.2: Metodologías de gestión de riesgos ya existentes.
Fuente: ISOTools Excellence (2014 b)

En las consideraciones que se tendrán posteriormente en este trabajo, será de aplicación la metodología MAGERIT que define el proceso de análisis y gestión de riesgos, elaborado por el Consejo Superior de Administración Electrónica[1] y que defiende que la gestión de los riesgos es clave en el éxito y buen gobierno de una entidad. Es también una de las metodologías propuestas para este fin por el Gobierno de España y en la página web oficial del mismo se puede descargar toda la documentación necesaria.

1 http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VWLsNU_tmkr

MAGERIT mantiene una relación directa con uso y control de las tecnologías de la información, admitiendo que esto supone un gran beneficio para los ciudadanos y las organizaciones pero haciéndonos conscientes en todo momento de que su uso conlleva a unos riesgos que deben ser minimizados con las medidas de seguridad necesaria para garantizar la total confianza de estos servicios.

MAGERIT permitirá medir los riesgos, permitiéndonos así saber cuánto valor estará en juego y cual es por tanto más importante proteger. Esta herramienta nos expondrá una metodología de medición completa que no dependa de la subjetividad de quien analiza. La forma de utilización será explicada posteriormente en la documentación propuesta requerida para completar el proceso de certificación.

1.4 BENEFICIOS DE UN SGSI

Algunos de los beneficios que se consiguen con la implantación de un SGSI son (ISOTools Excellence 2014a):

- Queda demostrado el compromiso de la alta dirección al cumplir con el sistema internacional más fiable en la gestión del riesgo relacionado con la información y la seguridad de la misma.

- La organización demostrará que ha tomado las opciones pertinentes a la hora de cumplir con la normativa legal que engloba la protección de datos y la seguridad de la información.

- La implantación de una metodología clara y estructurada ayudará a la organización a tomar decisiones fundamentadas en datos y estadísticas, por lo tanto aumentará su credibilidad hacia los empleados y terceras partes. Este aumento de confianza se traduce en unos mayores beneficios al aumentar el volumen de ventas o contrataciones.

- Mencionar por último la posibilidad de integrar otras certificaciones de gestión como ISO 9001 (sistema de gestión de calidad), ISO 14001 (sistema de gestión de medioambiental)u OHSAS 18001 (sistema de gestión de riesgos laborales).

1.5 ANÁLISIS DEL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

1.5.1 ¿QUÉ ES IT?

La tecnología de la información, o en inglés "Information Tecnology" (IT), se puede definir como un conjunto heterogéneo de herramientas, métodos y recursos tecnológicos empleados para crear, recabar, almacenar, gestionar y distribuir información (Burton 2000; Bologna y Walsh 1997).

Son muchas las empresas que, con el fin de asegurarse el mantenimiento de su hardware y software y la protección de sus datos, han solicitado de servicios IT desde los últimos 30 años. Pero en la última década el término de IT ha empezado a englobar conceptos que van mucho más allá del mantenimiento de equipos informáticos, tales como e-commerce (comercio electrónico), e-business (negocios y tiendas online), aplicaciones móviles, seguridad de la información y el revolucionario concepto de "la nube".

En el siglo XXI la prioridad del cliente es estar informado y conectado constantemente, tener acceso a la comunicación con personas en cualquier parte del mundo, poder ver un vídeo en tu dispositivo móvil o trabajar en equipo desde la distancia.

El sector de las tecnologías de la información ha desarrollado una importancia a nivel social que se hasta cierto punto se puede considerar una dependencia y que, se prevé que solo vaya en aumento en las próximas décadas.

1.5.2 MODELO DE LAS FUERZAS COMPETITIVAS DE PORTER

Para hacernos una idea del sector de la Tecnología de la Información, haremos un análisis del mismo basado en el modelo de Porter, que define las fuerzas que regulan la competencia y determinan la rentabilidad de un sector (Parra 2009). Dichas fuerzas son las siguientes (Porter 2003):

i. Amenaza de nuevos competidores.

ii. Poder de negociación con los clientes.
iii. Poder de negociación de los proveedores.
iv. Amenaza de productos o servicios sustitutivos.
v. Rivalidad entre empresas competidoras.

i) AMENAZA DE NUEVOS COMPETIDORES

Hace referencia a la posibilidad de que entren en juego dentro del sector empresas que venden el mismo tipo de producto u ofrecen el mismo servicio. En el momento en que un nuevo competidor entra en el sector, suele venir cargado de ideas novedosas que le permitan conseguir una cuota suficiente de mercado para poder alcanzar rentabilidad en un plazo apropiado. Pero el camino no es fácil, esta nueva empresa encontrará barreras de entrada, citando las siguientes:

- Falta de experiencia.

Donde consideramos desventajas que se adquieren con la práctica y el desempeño del negocio. Las economías de escala en la mayoría de casos traen la consecuencia de asumir unos costes de entrada poco ventajosos. La necesidad de capital supone también un obstáculo en la entrada, la inversión inicial tardará en recuperarse y se tiene que tener en cuenta la posibilidad de dar pérdidas durante los primeros meses.

- Desconocimiento de canales de distribución.

Es fundamentar garantizar la distribución de los servicios y productos que ofrece el nuevo agente.

- Lealtad de los clientes.

Si los servicios ofertados o los productos vendidos han obtenido la satisfacción del cliente, puede producirse un sentimiento de fidelidad ante el conformismo con el trato recibido que obviamente supone otro factor a tener en cuenta para las nuevas compañías que entran en el sector.

En el ámbito profesional, en el sector IT existen fuertes contratos entre las compañías que requieren de IT y las compañías que lo gestionan, esto crea una fuerte barrera de entrada para las nuevas compañías.

Cuanto menores sean estas barreras, mayor será la amenaza para la empresas del sector.

En España el sector IT fue durante mucho tiempo un monopolio, una sola compañía estatal ofertaba todos los servicios. Pero a principios de la década de 1990 la situación empezó a cambiar hasta llegar a la situación actual, en la que diferentes competidores ofertan servicios similares. Las posibilidades de supervivencia en el sector dependerán de las estrategias seguidas.

ii) PODER DE NEGOCIACIÓN CON LOS CLIENTES

Hace referencia a la capacidad que tienen los clientes para influir sobre nuestra empresa, podemos encontrar amenazas para nuestro sector cuando un grupo de clientes está bien organizado. Este grupo organizado tendrá el poder suficiente para ejercer presión sobre los precios, la cobertura del servicio o la calidad del mismo.

En el sector IT resulta difícil definir el término clientes en un sector tan extendido a nivel global como el de las tecnologías de la información, puesto que si nos referimos a cualquier usuario de las mismas, estaríamos considerando a casi toda la población mundial. Vamos a centrarnos en lo que puede considerarse el "cliente clave" en este sector, que son empresas con una red de tecnologías entre media y amplia, para cuya gestión es requerida la contratación de especialistas externos. El número de estas empresas es tan elevado actualmente, que se puede decir que el poder de negociación con los clientes es fuerte.

iii) PODER DE NEGOCIACIÓN DE LOS PROVEEDORES

Este factor explica la capacidad de los proveedores de imponer precios y condiciones, cuanto mejor organización dispongan mayor será su capacidad de influencia. Por ejemplo, cuanto menor sea la lista de proveedores o si el producto que venden está bien diferenciado, con mayor facilidad podrán aumentar su precio.

Es un aspecto a tener en cuenta en las pymes, ya que en términos generales no son consumidoras de grandes volúmenes de mercadería, por lo que pueden verse afectadas por el poder de los proveedores.

En el sector IT, los productos o servicios que entran en juego suelen ser muy similares aunque el proveedor varíe.

iv) AMENAZA DE PRODUCTOS O SERVICIOS SUSTITUTIVOS

Se refiere a la existencia o posible existencia de empresas que vendan los mismos productos (muy similares) o que oferten los mismos servicios.

Esto produce limitaciones en el precio que el cliente está dispuesto a pagar fijando un valor tope en el mismo. Por lo tanto el precio sufre limitaciones, y a excepción de que se introduzca una mejora en la calidad o se genere alguna diferenciación o mejora no podrá aumentarse porque conllevaría a una reducción de sus beneficios.

v) RIVALIDAD ENTRE EMPRESAS COMPETIDORAS

Es el resultado de las cuatro anteriores, se refiere a las empresas que compiten directamente entre sí dentro de un mismo sector bien industrial o bien de servicios.

El sector IT se caracteriza por su rápida capacidad de cambio y crecimiento, siempre dependiendo de nuevas ideas o mejoras. La razón por la que la entrada en el sector de nuevos competidores fracasa, es precisamente por la fuerte rivalidad entre los ya existentes.

Lo más habitual es que dentro de un sector se genere una competencia por conseguir una posición privilegiada dentro del mismo, la intensidad de la rivalidad dependerá de diversos factores, algunos de ellos son:

- La cantidad de competidores, su poder y su tamaño. Siendo los más poderosos los que suelen ser considerados rivales más fuertes.

- La capacidad de acción de las mismas, una misma idea o estrategia puede causar menor o mayor impacto según como sea ejecutada. El personal y la dirección de la entidad serán quienes tengan en sus manos el poder de que un movimiento triunfe o fracase.

- El producto o servicio no ofrece características de diferenciación, será un impedimento para todo el sector a la hora de elaborar estrategias comerciales.

- Los producto o servicios, pese a ser de un mismo sector, son completamente diferentes. La rivalidad entre las mismas no será considerada como tal.

CAPÍTULO 2

ISO/IEC 27001

2.1 LA SERIE 27000

La serie de normas *ISO/IEC 27000* es un conjunto de estándares que definen las mejores prácticas para que cualquier organización pública o privada, indiferentemente de su tamaño o área de actividad, pueda desarrollar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información.

Algunas de estas normas de esta familia de estándares son:

ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary.
ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security management.
ISO/IEC 27003: Information security management system implementation guidance.
ISO/IEC 27004: Information security management — Measurement.
ISO/IEC 27005: Information security risk management.
ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems.
ISO/IEC 27007: Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27035: Information technology – Security techniques – Information security incident management.
ISO/IEC 27799: Information security management in health using *ISO/IEC 27002*.

2.2 UNA INTRODUCCIÓN A LA NORMA ISO/IEC 27001:2013

La norma *ISO 27001* especifica los requisitos para la creación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier tipo de organización sin importar su tamaño ni el sector en el que se encuentre.

Mediante la certificación en esta norma se podrá demostrar de cara a clientes y accionistas que toda la información garantiza las tres siguientes dimensiones de la seguridad:

- **Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados [*UNE-ISO/IEC 27001:2007*]. Su objetivo es controlar que el acceso a la información estará restringido, solo podrán acceder a la misma las personas autorizadas. Implica una lucha contra las filtraciones de información y los accesos no autorizados a la misma.

- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [*ISO/IEC 13335-1:2004*]. Su objetivo es garantizar que los métodos de procesamiento de información son exactos, y asegura unos datos completos y correctos. Será prioritario evitar una información incompleta, que haya sido corrupta o manipulada.

- **Disponibilidad**: Propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [*UNE 71504:2008*]. Su objetivo es controlar que tan sólo las personas físicas autorizadas podrán acceder a la información cuando lo soliciten o sea necesario.

Cualquier debilidad en alguna de estas tres dimensiones supondrá una amenaza para la organización. Una garantía del buen uso y protección de la información reducirá los riesgos, permitirá cumplir con la legislación y los reglamentos vigentes y causará también impacto positivo en la imagen corporativa de la organización.

La *ISO/IEC 27001:2013 (ISO 2013)*, cuya versión española es *ISO/IEC 27001:2014* (AENOR 2014), es la primera revisión de la *ISO/IEC 27001:2005 (ISO 2005)*, cuya versión española es *ISO/IEC 27001:2007* (AENOR 2007). La nueva versión se caracteriza principalmente por ofrecer mayor flexibilidad de implementación. Además, ofrece una mayor homogeneidad en su estructura con respecto a otros estándares ISO, lo que permitirá, si es oportuno, obtener otras certificaciones relacionadas (Calidad, Medio Ambiente…) que tendrán múltiples documentos en común.

2.3 UN RECORRIDO POR LA NORMA ISO/IEC 27001:2013

La ISO 27001:2013 está estructurada en las siguientes cláusulas con el Ciclo de Deming: Planificar-Hacer-Comprobar- Actuar o ciclo PDCA (ver Figura 2.1):

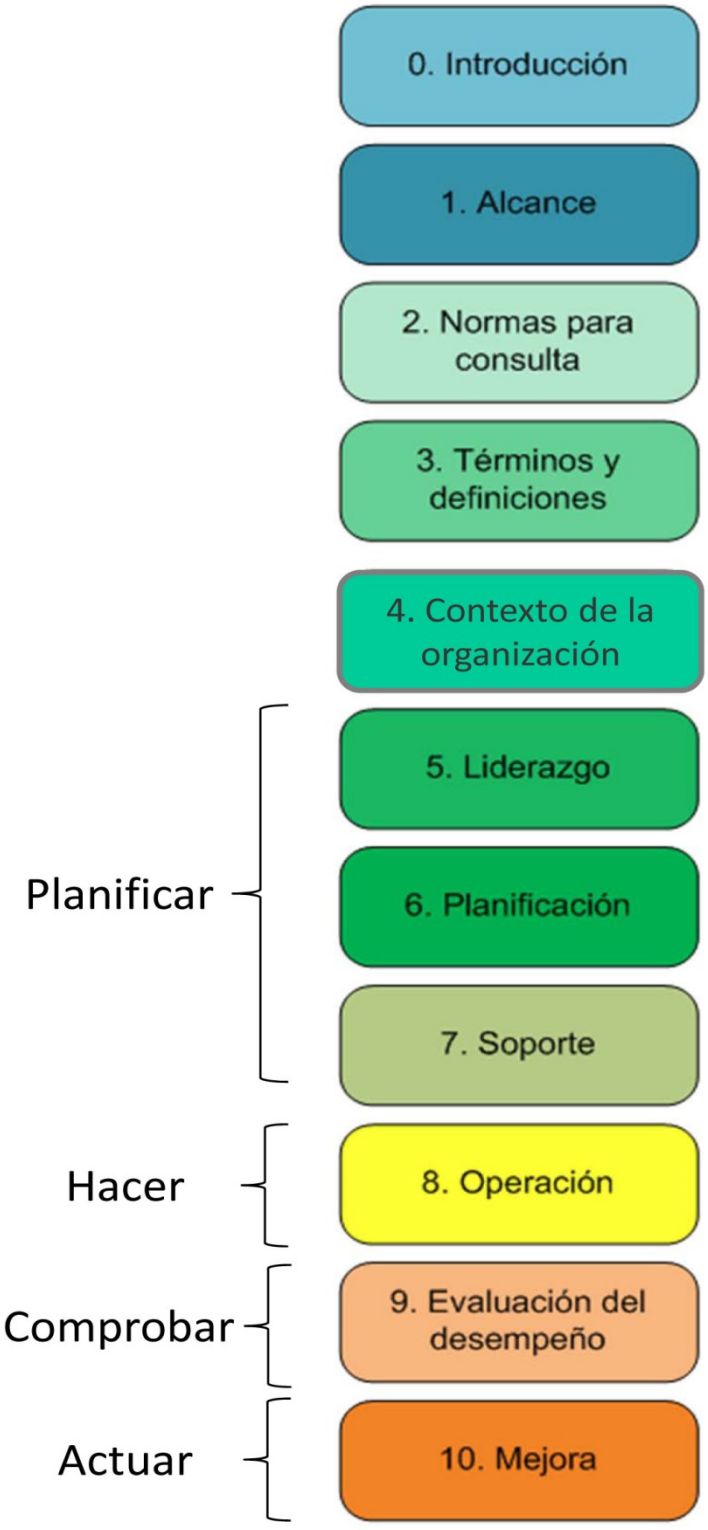

Figura 2.1: Diagrama de la estructura estándar de ISO/IEC 27001:2013.
Fuente: AENOR (2014)

Cláusula 0: Introducción

En su primer párrafo nos explica la razón de ser de esta norma, indicando con claridad que se busca el establecimiento, implementación, mantenimiento y mejora continua de un SGSI. En esta cláusula se dice de forma explícita que la adopción de un SGSI es una decisión estratégica de la organización, pero esta podrá hacerse de forma global mediante cualquier método sin obligar a un PDCA en ningún momento.

Se especifican los tres compromisos de la seguridad de la información, preservación de su confidencialidad, integridad y disponibilidad.

El SGSI deberá ajustarse a las necesidades de la organización. Esta norma demostrará la capacidad de la organización para cumplir con los requisitos establecidos en la seguridad de la información y podrá ser utilizado por partes internas y externas.

Esta cláusula también nos indica que el orden en el que son presentados los requisitos no refleja ni su importancia ni el orden que deben ser implementados.

Cláusula 1: Objeto y campo de aplicación

Independientemente del tipo, tamaño o naturaleza de la organización, los requisitos en esta norma internacional son genéricos y se pueden aplicar a cualquier organización.

Será obligatorio cumplir los requisitos especificados en los capítulos 4 al 10 para obtener la declaración de conformidad y poder certificarse.

Cláusula 2: Normas para consulta

La norma *ISO/IEC 27000*, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario. Se convierte en la única referencia normativa de consulta obligatoria.

Cláusula 3: Términos y Definiciones

Para cualquier consulta en los términos nos derivan a la norma mencionada anteriormente, *ISO/IEC 27000.*

Cláusula 4: Contexto de la Organización

En esta cláusula se centra en identificar quienes son los beneficiarios de SGSI, nos propone las pautas y puntos de vista que se debe plantear la organización para la correcta identificación de los mismos. En la Figura 2.2 se recoge la secuencia actividades de este proceso, las cuales se agrupan en las siguientes sub-cláusulas:

Sub-cláusula 4.1. Compresión de la organización y de su contexto:

> Hace referencia en la importancia de identificar apropiadamente las circunstancias internas y externas que afectan a la organización ya que es vital para el correcto progreso ser conscientes de nuestro modelo y de su entorno.
>
> Se establecerán todas las posibles causas internas o externas que estén incluidas en el ámbito de la organización y que puedan afectar en mayor o menor medida a los resultados del SGSI.

Sub-cláusula 4.2. Compresión de las necesidades y expectativas de las partes interesadas:

> Se introduce el concepto de "Las partes interesadas", será necesario determinar cuáles de ellas son relevantes y cuales son los requisitos que estas mismas establecerán para con la entidad, siempre que estén relacionados con SGSI.

Sub-cláusula 4.3. Determinación del alcance del sistema de gestión de seguridad de la información:

> En el alcance se describirán los puntos previamente mencionados y se detallarán que actividades lleva a cabo la organización y cuales son realizadas por terceros. El alcance deberá estar disponible como información documentada.

Sub-cláusula 4.4. Sistema de gestión de seguridad de la información:

De nuevo se recuerda la importancia de establecer, implementar, mantener y mejorar la mejora continua.

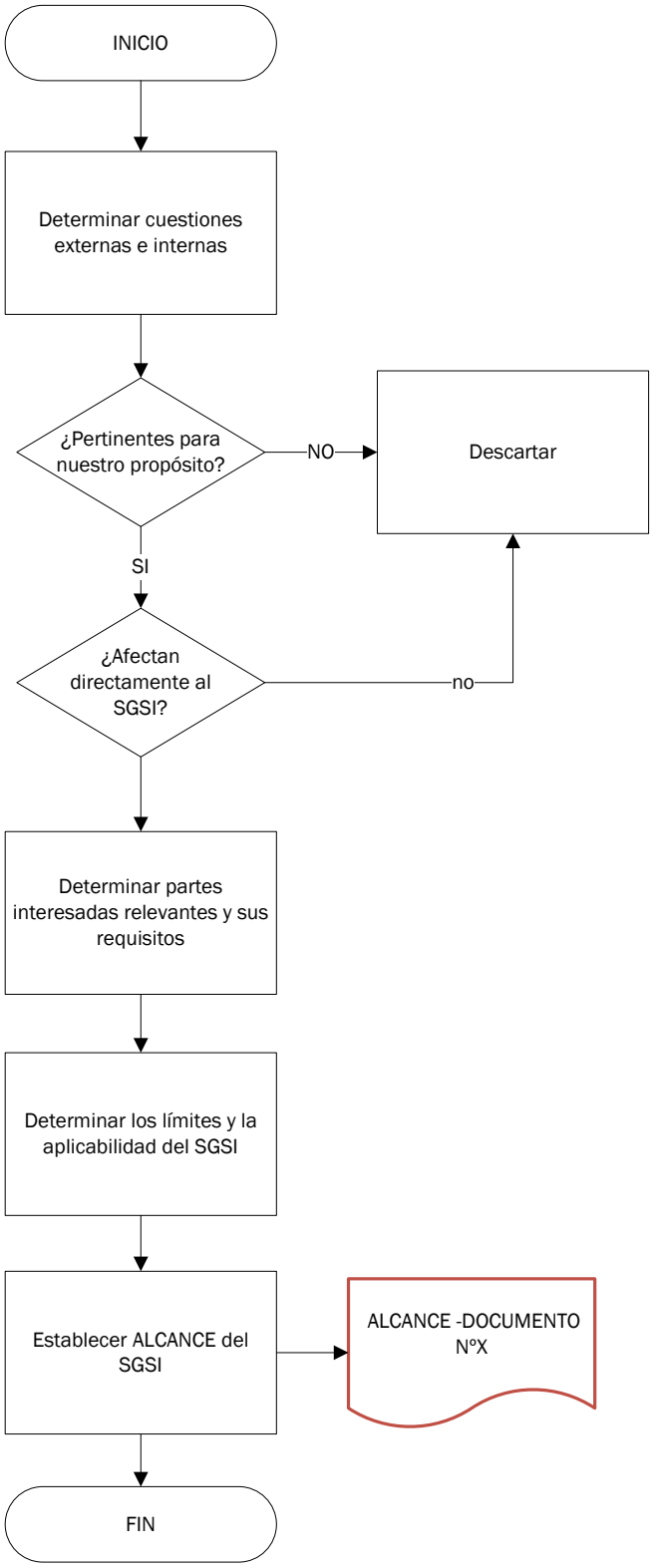

Figura 2.2: Diagrama propuesto para la Cláusula 4: Contexto de la organización ISO/IEC 27001:2013. Fuente: Elaboración propia

Cláusula 5: Liderazgo

En esta cláusula se definen los aspectos que definen al SGSI como un proceso estratégico de la organización y establece el comportamiento que deberá de tomar la alta dirección con respecto al SGSI.

Se detallan los procedimientos a seguir por la alta dirección en tres sub-cláusulas:

Sub- cláusula 5.1. Liderazgo y compromiso:

La figura de la alta dirección será responsable de:

- asegurar que se establece una política y se definan unos objetivos de seguridad de la información,
- se integren los requisitos del sistema y se pondrán a disposición los recursos necesarios (económicos, tecnológicos, etcétera).
- asegurar la correcta implementación del SGSI.

La gestión de las personas será igualmente importante, comunicando a cuantos integran la organización la importancia de seguir el SGSI.
Se buscará que el SGSI alcance los resultados previstos y se siga un proceso de mejora continua.

Sub- cláusula 5.2.Política:

Se reafirma el compromiso de la alta dirección, que será responsable de definir una política que en todo momento se adecúe a los propósitos de la organización, se incluirán en ella los objetivos de seguridad de la información (o un marco de referencia para el establecimiento de los objetivos), se describirán los compromisos de cumplir con los requisitos y de cumplir con la mejora continua. La política deberá estar disponible como información documentada.

Sub- cláusula 5.3 Roles, responsabilidades y autoridades en la organización:

Se nombrarán los roles pertinentes para garantizar que las responsabilidades y autoridades relacionadas con el SGSI sigan buenas prácticas que cumplan en todo momento la norma internacional y que se comuniquen sobre el estado del SGSI.

Cláusula 6: Planificación

Esta sección es clave en la creación y mantenimiento del SGSI. Se enfoca en detallar el proceso para la evaluación de riesgos, la detección de oportunidades y la definición de los objetivos de seguridad.

Antes de seguir, es necesario definir los siguientes conceptos en relación con la apreciación y tratamiento de los riesgos, de acuerdo con la metodología MAGERIT para la mejora continua:

- **Amenazas**, causa potencial de un incidente que puede causar daños a un sistema de información o a una organización

- **Salvaguardas:** que son medidas de protección desplegadas para que aquellas amenazas no causen daño o causen el menor posible.

Sub-cláusula 6.1. Acciones para tratar los riesgos y oportunidades:

Esta sub cláusula en divide, a su vez, en los siguientes tres apartados a los cuales hay que prestar mucha atención. En la Figura 2.3 se recoge la secuencia de actividades de este proceso, las cuales se agrupan en las siguientes sub-cláusulas:

Sub-cláusula 6.1.1.Consideraciones generales:

En las consideraciones generales se tendrán las cuestiones a las que se hace referencia en la cláusula 4 (4.1 y 4.2). Se determinarán los riesgos y oportunidades a tratar con el fin de que:

- Sea posible garantizar el resultado que se ha previsto con la implantación del SGSI
- Evitar y prevenir eventos no deseados
- Obtener una mejora continua.

Sub-cláusula 6.1.2. Apreciación de riesgos de seguridad de la información:

En la apreciación de riesgos se indican las siguientes ideas principales:

- Se establecen criterios de aceptación del riesgo y criterios para llevar a cabo las apreciaciones de los riesgos.
- Los resultados de la evaluación de riesgos serán consistentes, válidos y comparables.
- Necesidad de identificación de los riesgos como cualquier acción que implique una posible pérdida de confidencialidad, integridad y disponibilidad de la información. Identificación de los dueños de los riesgos. El concepto de "dueño del riesgo" es muy variable ya que dentro de un sector IT no tiene por qué afectar a un responsable en concreto, si no que puede ser un área en concreto de la organización.
- Será necesario estudiar los riesgos a fondo, valorando: consecuencias si se da el suceso, valoración de la probabilidad de ocurrencia y el nivel de riesgo que supone cada uno.
- Evaluación de los riesgos de seguridad de la información identificados mediante la comparación de los resultados que obtenemos con los criterios establecidos previamente.

La organización tendrá disponible como información documentada todo el proceso de apreciación de riesgos.

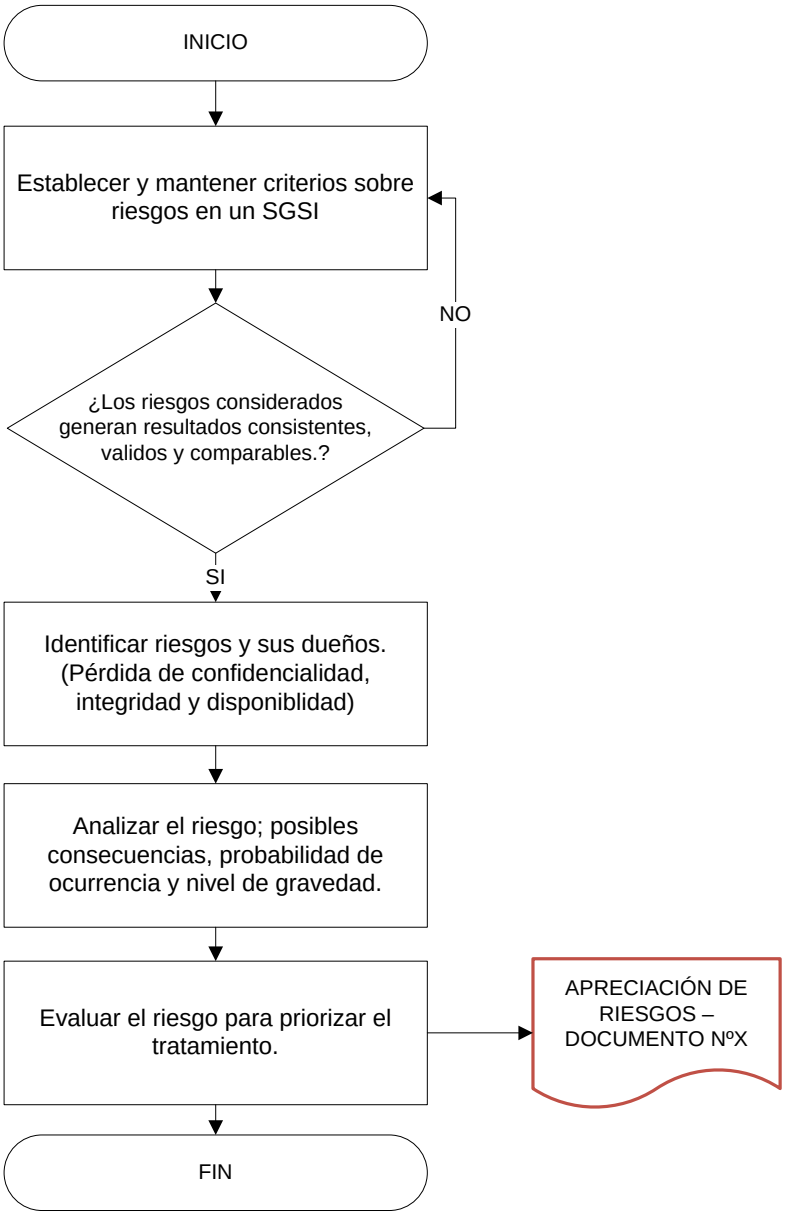

Figura 2.3: Diagrama propuesto para la Cláusula 6.1.2: Apreciación de riesgos de seguridad de la información. ISO/IEC 27001:2013. Fuente: Elaboración propia

Sub-cláusula 6.1.3. Tratamiento de los riesgos de seguridad de la información:

Se hace referencia a la importancia de definir controles para tratar los riesgos de seguridad de la información. Estos controles pueden adaptarse según las necesidades de la organización teniendo en cuenta que los controles de referencia recogidos en el Anexo A son necesarios y no debemos olvidar ninguno. En la Figura 2.4 se recoge la secuencia de actividades de este proceso.

Se crea el documento "Declaración de Aplicabilidad" (también llamado en muchos casos con sus siglas en inglés SOA 'Statement of applicability'). Que consiste en una declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo. En este documento se recogerán las justificaciones de uso o de exclusión de los controles del Anexo A.

Se elabora un plan de tratamiento de riesgos que tendrá que ser aprobado por los dueños de los riesgos. Este plan se realiza cuando la organización se cuestiona si cumple con todos los controles propuestos en el Anexo A. con vistas a que quede determinada la "Declaración de Aplicabilidad" (ver tabla 2.1). Cada cláusula y sub-cláusula en el Anexo A, quedarán recogidas con su control correspondiente y la organización reflexionará si ese control se cumple respondiendo a preguntas al respecto, que pueden modificarse en función de las necesidades de la organización, su respuesta puede ser afirmativa, negativa o no aplicable (SI, NO o N/A), en el comentario se recogerá lo que sea necesario para esclarecer su respuesta.

Tabla 2.1: Plantilla de los controles propuestos en función del anexo A para elaborar la "Declaración de aplicabilidad".

TEST INICIAL – Declaración de Aplicabilidad					
GRUPO	ID	CONTROL	PREGUNTA	RESPUESTA	COMENTARIOS
Cláusula	Sub-cláusula				

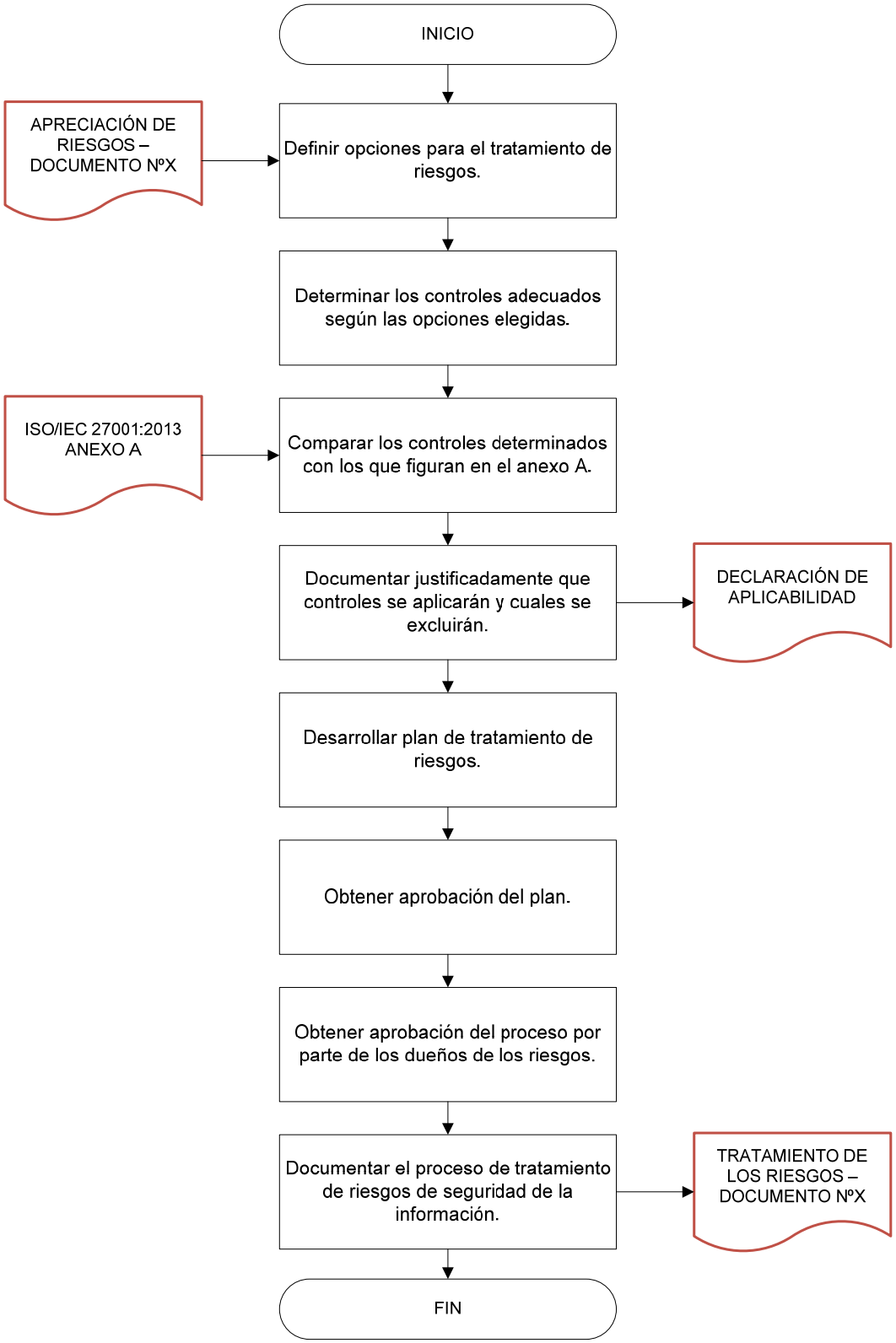

Figura 2.4: Diagrama propuesto para la Cláusula 6.1.3: Tratamiento de los riesgos de seguridad de la información. ISO/IEC 27001:2013. Fuente: Elaboración propia

Todo el proceso de tratamiento de los riesgos de seguridad de la información, estará disponible como información documentada.

Sub-Cláusula 6.2. Objetivos de seguridad de la información y planificación para su consecución:

Quedan definidas las características que deben tener los objetivos de seguridad de la información: coherencia, posibilidad de medición, acordes con el SGSI y que tengan la posibilidad de ser comunicados y actualizados (Figura 2.5). Los objetivos estarán disponibles como información documentada. Así mismo la organización establecerá un plan para la consecución de los objetivos.

Figura2.5: Características de los objetivos de seguridad de la información. ISO/IEC27001:2013. Fuente: Elaboración propia

Cláusula 7: Soporte

En esta cláusula encontramos las referencias a los medios que serán necesarios en la organización para alcanzar el desarrollo completo de un SGSI. Se hace también hincapié en la importancia de los recursos humanos, las capacidades de cada persona que forma parte de la organización, insistiendo en su concienciación y formación para asegurar un buen desempeño del sistema de seguridad de la información.

Dentro de este apartado encontramos también una descripción de la forma en que se deberá tratar la información documentada de la organización, desde su creación y accesibilidad hasta su protección.

Sub-Cláusula 7.1. Recursos:

Los recursos a aportar deberán asegurar el establecimiento, implementación y mejora del SGSI. Cuando organización decide implementar el SGSI y buscar la certificación, se trata sin duda de una decisión estratégica importante y por lo tanto poner al alcance los recursos necesarios para su correcta ejecución será imprescindible.

Sub-Cláusula 7.2. Competencia:

Sobre la ya mencionada importancia de las personas, en esta cláusula se hace referencia a las competencias y aptitudes de las mismas. El equipo encargado de la gestión del SGSI debe disponer de un nivel de conocimientos suficiente como para poder hacer frente a su tarea y estarán dispuestos a adquirir las competencias necesarias en caso de carecer de ellas.
La organización podrá optar por mecanismos de formación de personal en los casos en que sea necesario adquirir una nueva competencia. La evidencia de la competencia del personal estará disponible como información documentada.

Sub-Cláusula 7.3. Concienciación:

Todos los empleados deberán: ser conscientes de la política de seguridad, de su contribución a que el SGSI sea eficaz y lo que puede implicar incumplir con los requisitos definidos.

Sub-Cláusula 7.4. Comunicación:

La comunicación será fundamental en la organización tanto a nivel interno como externo. En las comunicaciones quedará claro su contenido y responderá siempre a las preguntas de cuándo, a quién y quién comunicará. Se describirán también la forma en que se transmitirá dicha información.

La importancia de esta cláusula reside en que, en el caso de una mala práctica o incidencia, se requerirá toda la información posible para minimizar los daños y el tiempo de respuesta.

Sub-Cláusula 7.5. Información Documentada:

El control de la documentación se estructura en las siguientes categorías (ver Figura 2.6): consideraciones generales, creación y actualización, y control.

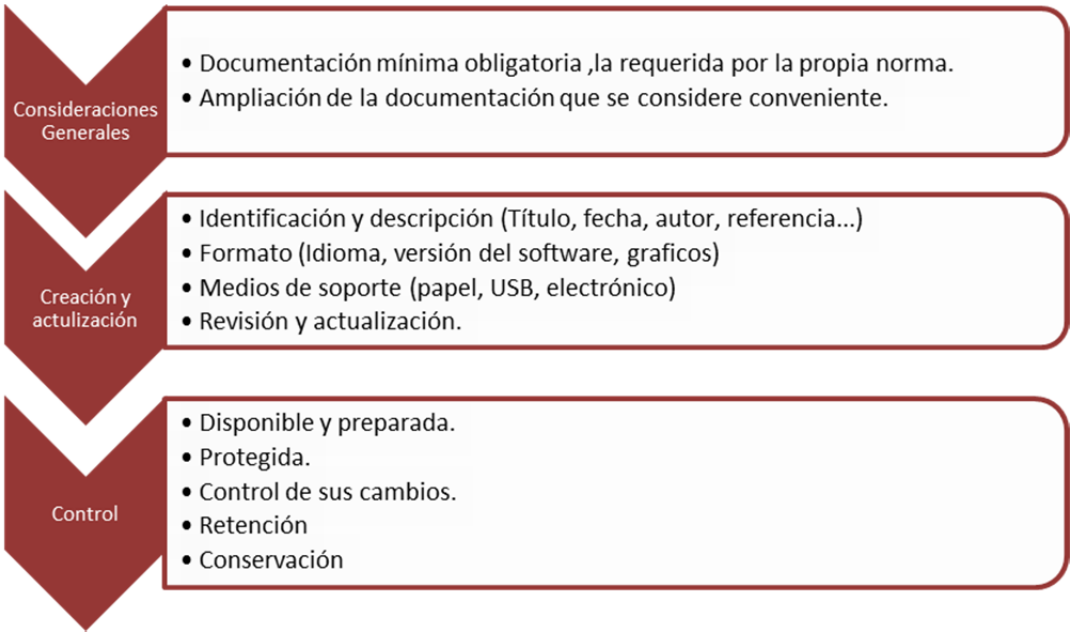

Figura 2.6: Información en la Organización. Resumen de la cláusula 7.5. Información Documentada. ISO/IEC 27001:2013. Fuente: Elaboración propia

Consideraciones generales: Habrá una documentación mínima obligatoria que es la requerida por la propia norma y se expone que, a criterio de la propia organización, se podrá ampliar la documentación que se considere conveniente según sus necesidades siempre y cuando ayude a la eficacia del SGSI. El volumen de información que será manejado variará de una empresa a otra y dependerá directamente de factores como: el tamaño de la organización, su tipo de actividad, la complejidad de sus procesos y la competencia de los trabajadores.

Creación y actualización de la información documentada: La documentación deberá será creada y actualizada, en ella siempre figurará: una identificación y descripción, el formato y el soporte. Será revisada para mantenerse actualizada.

Control de la información documentada: La información requerida por el SGSI asegurará una información disponible y accesible en cualquier

momento, que contará con la protección apropiada. Además para garantizar el control de la información documentada se tratará, cuando sea necesario: el control de cambios, retención y disposición. La información cuyo origen no provenga del interior de la organización pero que sea necesaria para cualquier ámbito del SGSI se identificará y controlará como si de información propia se tratase.

Cláusula 8: Operación

Esta cláusula se centrará en explicar cómo se asegurará un correcto funcionamiento de SGSI una vez implementado dentro de la organización.

Sub-cláusula 8.1. Planificación y control operación:

Se determina que la organización deberá planificar, implementar y controlar los procesos necesarios para asegurar los requisitos y para implementar la sub-cláusula 6.1 *Acciones para tratar los riesgos y oportunidades*. La organización se encargará también de implementar los planes necesarios para alcanzar lo propuesto en la sub-cláusula 6.2 *Objetivos de seguridad de la información y planificación para su consecución*.

La información expuesta previamente estará disponible como información documentada con el fin de tener la certeza de que los procesos se están llevando a cabo de forma apropiada, la organización revisará y cuando sea necesario, modificará los puntos que considere. Las consecuencias producidas tanto por los cambios planificados como por los no planificados serán tenidas en cuenta en todo momento para mitigar los efectos adversos.
Se asegura también un control de los procesos contratados externamente.

Sub-cláusula 8.2. Apreciación de los riesgos de seguridad de la información:

Especifica la necesidad de que se efectúen apreciaciones de los riesgos a intervalos planificados o en el caso de que realicen modificaciones, siguiendo los criterios definidos en la sub-cláusula 6.1.2 *Apreciación de riesgos de seguridad de la información*.

Los resultados de estas apreciaciones estarán disponibles como información documentada.

Sub-cláusula 8.3. Tratamiento de los riesgos de seguridad de la información:

Conforme se vayan alcanzando resultados y conclusiones sobre los riesgos, la organización irá adaptándose a los nuevos criterios.

Los resultados alcanzados estarán disponibles como información documentada.

Cláusula 9: Evaluación de desempeño

El análisis de los resultados en comparación con los objetivos y las metas a cumplir (definidas en la sub-cláusula 6.2 *Objetivos de seguridad de la información y planificación para su consecución*,) es muy importante en un SGSI. Mediante esta cláusula plantearemos medios de análisis para comprobar si dichos objetivos se están cumpliendo o no.

Sub-cláusula 9.1. Seguimiento, medición, análisis y evaluación

Para evaluar el desempeño y la eficacia del SGSI, se debe determinar:

- Qué es necesario medir y monitorizar, incluyendo procesos y controles de seguridad de la información.
- Que métodos de seguimiento, medición, análisis y evaluación se están aplicando, según sea necesario, para respaldar unos resultados óptimos.
- Cuándo se realizarán seguimientos y mediciones.
- Quién llevará a cabo los seguimientos y mediciones.
- Cuándo se analizarán los resultados obtenidos en las mismas.
- Quién será el responsable de esta evaluación.

Esta evaluación de desempeño estará disponible como información documentada.

Sub-cláusula 9.2. Auditoría interna

Las auditorías internas temporales son las herramientas necesarias para verificar y extraer toda la información necesaria sobre el estado y

funcionamiento el SGSI en la organización. Una auditoría interna asegurará que el SGSI:

- Cumple con: los requisitos propios de la organización y los requisitos de la norma internacional.
- Cuenta con una implementación y mantenimiento eficaz.

Para esto la organización debe planificar, establecer, implementar y mantener los programas de auditoría necesarios.

Estos programas de auditoría compartirán las siguientes características:

- Incluyen la frecuencia de las mismas, los métodos, responsabilidades, requisitos de planificación y la elaboración de informes.
- Tienen en cuenta la importancia de los procesos que entran en juego y los resultados de las auditorías realizadas con anterioridad.
- Definen los criterios y el alcance.
- Los auditores seleccionados son reflejo de objetividad e imparcialidad.
- Se informa de los resultados a la alta dirección

Todo el proceso referente a las auditorías internas, estará disponible como información documentada

Sub-cláusula 9.3. Revisión por la dirección

Es fundamental que la alta dirección esté involucrada en todo el proceso, supervisando la toma de decisiones y las posibles modificaciones en lo que respecta al SGSI. Es necesario que, a intervalos previamente planificados, la alta dirección revise el sistema de gestión completo. Estas revisiones tendrán en consideración:

- El estado desde la última revisión.
- Los cambios (internos o externos) que afecten al SGSI.
- Información sobre el desempeño de la seguridad de la información incluyendo datos y sus interpretaciones sobre:
    - No conformidades y acciones correctivas.

  - Resultados de las acciones monitorizadas y medidas.
  - Resultados de las auditorías.
  - Cumplimiento de los objetivos de la seguridad de la información.
- Consideración de las opiniones de las partes interesadas.
- Resultados del plan de apreciación de riesgos y el estado del plan de tratamiento.
- Oportunidades de mejora continua.

La salida que genere la alta dirección incluirá las decisiones que tengan que ver con las oportunidades de mejora continua y necesidades de cambios en el SGSI. Esta salida estará disponible como información documentada

Cláusula 10: Mejora

A lo largo de todo el proceso se hace referencia en múltiples ocasiones a la importancia de la mejora en el proceso relativo al SGSI. En esta cláusula se especifican métodos para tratar cuando se encuentre una pauta susceptible de mejora en el sistema.

Sub-cláusula 10.1.No conformidad de acciones correctivas

Ante la aparición de una no conformidad:

- Reaccionar con acciones que la mitiguen y corrijan y con disposición a hacer frente a las consecuencias.
- Evaluar las mejores opciones que se puedan llevar a cabo para evitar que vuelva a suceder la causa de la no conformidad. Para esto se propone: revisión de la no conformidad, determinación de las causas, comparativa con otras no conformidades similares u otras que puedan ocurrir.
- Realizar la acción necesaria.
- Revisar que las acciones correctivas llevadas a cabo sean eficientes.
- Aplicar cambios, cuando proceda, en el SGSI.

Las acciones correctivas deberán adecuarse a los efectos de las no conformidades que aparezcan.

Este proceso estará disponible como información documentada y será el registro de las no conformidades encontradas, de las acciones llevadas a cabo para su corrección y de los resultados posteriores a las mismas.

Sub-cláusula 10.2. Mejora continua

Es una responsabilidad fundamental de la organización asegurar una mejora continua en la idoneidad, adecuación y eficacia del SGSI. Cada revisión del mismo deberá consolidar con resultados tangibles este compromiso.

Anexo A: Objetivos de control y controles de referencia

En este anexo A se incluye una lista de 114 controles necesarios y sus objetivos, expuestos en 14 categorías de control, de la 5 a la 18. Se espera el uso de este anexo en lo referente a la Declaración de Aplicabilidad definida en la cláusula 6.1.3.

ISO/IEC 27001:2013 ANEXO A DESGLOSE PARA USO DIDÁCTICO

A.5 Políticas de Seguridad de la Información
- 5.1 Directrices de gestión de la Seguridad de la Información
  - A.5.1.1 Políticas para la Seguridad de la Información
  - A.5.1.2 Revisión de las Políticas para la Seguridad de la Información

A.6 Organización de la Seguridad de la Información
- 6.1 Organización Interna
  - A.6.1.1 Roles y responsabilidades en seguridad de la información
  - A.6.1.2 Segregación de tareas
  - A.6.1.3 Contacto con las autoridades
  - A.6.1.4 Contacto con grupos de interés especial
  - A.6.1.5 Seguridad de la información en la gestión de proyectos
- 6.2 Los dispositivos móviles y el teletrabajo
  - A.6.2.1 Política de dispositivos móviles
  - A.6.2.2 Teletrabajo

A.7 Seguridad relativa a los recursos humanos
- 7.1 Antes del empleo
  - A.7.1.1 Investigación de antecedentes
  - A.7.1.2 Términos y condiciones del empleo
- 7.2 Durante el empleo
  - A.7.2.1 Responsabilidades de gestión
  - A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
  - A.7.2.3 Proceso disciplinario
- 7.3 Finalización del empleo o cambio en el puesto de trabajo
  - A.7.3.1 Responsabilidades ante la finalización o cambio

A.8 Gestión de Activos
- 8.1 Responsabilidad sobre los activos
  - A.8.1.1 Inventario de activos
  - A.8.1.2 Propiedad de los activos
  - A.8.1.3 Uso aceptable de los activos
  - A.8.1.4 Devolución de activos
- 8.2 Clasificación de la Información
  - A.8.2.1 Clasificación de la información
  - A.8.2.2 Etiquetado de la información
  - A.8.2.3 Manipulado de la información
- 8.3 Manipulación de los soportes
  - A.8.3.1 Gestión de soportes extraíbles
  - A.8.3.2 Eliminación de soportes
  - A.8.3.3 Soportes físicos en tránsito

A.9 Control de Acceso
- 9.1 Requisitos del negocio para el control de acceso
  - A.9.1.1 Política de control de acceso
  - A.9.1.2 Acceso a las redes y a los servicios de red
- 9.2 Gestión de acceso de usuario
  - A.9.2.1 Registro y baja de usuarios
  - A.9.2.2 Provisión de acceso de usuario
  - A.9.2.3 Gestión de privilegios de acceso
  - A.9.2.4 Gestión de la información de secreta de autenticación de los usuarios
  - A.9.2.5 Revisión de los derechos de acceso de usuario
  - A.9.2.6 Retirada o reasignación de los derechos de acceso
- 9.3 Responsabilidades del usuario
  - A.9.3.1 Uso de la información secreta de autenticación
- 9.4 Control de acceso a sistemas y aplicaciones
  - A.9.4.1 Restricción del acceso a la información
  - A.9.4.2 Procedimientos seguros de inicio de sesión
  - A.9.4.3 Sistema de gestión de contraseñas
  - A.9.4.4 Uso de utilidades con privilegiados del sistema
  - A.9.4.5 Control de acceso al código fuente de los programas

A.10 Criptografía
- 10.1 Controles Criptográficos
  - A.10.1.1 Política de uso de los controles criptográficos
  - A.10.1.2 Gestión de claves

A.11 Seguridad Física y del entorno
- A.11.1 Áreas seguras
  - A.11.1.1 Perímetro de seguridad física
  - A.11.1.2 Controles de físicos de entrada
  - A.11.1.3 Seguridad de oficinas, despachos y recursos
  - A.11.1.4 Protección contra las amenazas externas y ambientales
  - A.11.1.5 El trabajo en áreas seguras
  - A.11.1.6 Áreas de carga y descarga
- A.11.2 Seguridad de los equipos
  - A.11.2.1 Emplazamiento y protección de equipos
  - A.11.2.2 Instalaciones de suministro
  - A.11.2.3 Seguridad del cableado
  - A.11.2.4 Mantenimiento de los equipo
  - A.11.2.5 Retirada de materiales propiedad de la empresa
  - A.11.2.6 Seguridad de los equipos fuera de las instalaciones.
  - A.11.2.7 Reutilización o eliminación segura de equipos
  - A.11.2.8 Equipo de usuario desatendido
  - A.11.2.9 Política de puesto de trabajo despejado pantalla limpia

A.12 Seguridad de las Operaciones
- A.12.1 Procedimientos y responsabilidades operacionales
  - A.12.1.1 Documentación de procedimientos de operación.
  - A.12.1.2 Gestión de cambios
  - A.12.1.3 Gestión de capacidades
  - A.12.1.4 Separación de los recursos de desarrollo, prueba y operación
- A.12.2 Protección contra el software malicioso (malware)
  - A.12.2.1 Controles contra el código malicioso

- A.12.3 Copias de seguridad
  - A.12.3.1 Copias de seguridad de la información
- A.12.4 Registros y supervisión
  - A.12.4.1 Registro de Eventos
  - A.12.4.2 Protección de la información de registro
  - A.12.4.3 Registros de administración y operación
  - A.12.4.4 Sincronización del Reloj
- A.12.5 Control del software en explotación
  - A.12.5.1 Instalación de software en explotación
- A.12.6 Gestión de la vulnerabilidad técnica
  - A.12.6.1 Gestión de las vulnerabilidades técnicas
  - A.12.6.2 Restricciones en la instalación de software
- A.12.7 Consideraciones sobre la auditoría de sistemas de información
  - A.12.7.1 Controles de auditoría de sistemas de información

A.13 Seguridad de las Comunicaciones
- A.13.1 Gestión de la seguridad de redes
  - A.13.1.1 Controles de red
  - A.13.1.2 Seguridad de los servicios de red
  - A.13.1.3 Segregación en redes
- A.13.2 Intercambio de información
  - A.13.2.1 Políticas y procedimientos de intercambio de información
  - A.13.2.2 Acuerdos de intercambio de información
  - A.13.2.3 Mensajería electrónico
  - A.13.2.4 Acuerdos de confidencialidad o no revelación

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información
- A.14.1 Requisitos de seguridad en sistemas de información
  - A.14.1.1 Análisis de requisitos y especificaciones de Seguridad de la información
  - A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas
  - A.14.1.3 Protección de las transacciones de servicios de aplicaciones
- A.14.2 Seguridad en el desarrollo y en los procesos de soporte
  - A.14.2.1 Política de desarrollo seguro
  - A.14.2.2 Procedimiento de control de cambios en sistema
  - A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
  - A.14.2.4 Restricciones a los cambios en los paquetes de software
  - A.14.2.5 Principios de ingeniería de sistemas de seguros
  - A.14.2.6 Entorno de desarrollo seguro
  - A.14.2.7 Externalización del desarrollo de software
  - A.14.2.8 Pruebas funcionales de seguridad del sistema
  - A.14.2.9 Pruebas aceptación de sistema
- A.14.3 Datos de prueba
  - A.14.3.1 Protección de los datos de prueba

A.15 Relación con Proveedores
- 15.1 Seguridad en las relaciones con los proveedores
  - A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores
  - A.15.1.2 Requisitos de seguridad en contratos con terceros
  - A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
- 15.2 Gestión de la provisión de servicios del proveedor
  - A.15.2.1 Control y revisión de la provisión de servicios del proveedor
  - A.15.2.2 Gestión cambios en la provisión del servicio del proveedor

A.16 Gestión de Incidentes de Seguridad de la Información
- A.16.1 Gestión de incidentes de seguridad de la información y mejoras
  - A.16.1.1 Responsabilidades y procedimientos
  - A.16.1.2 Notificación de los eventos de seguridad de la información
  - A.16.1.3 Notificación de puntos débiles de seguridad
  - A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
  - A.16.1.5 Respuesta a incidentes de seguridad de la información
  - A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
  - A.16.1.7 Recopilación de evidencias

A.17 Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio
- A.17.1 Continuidad de la seguridad de la Información
  - A.17.1.1 Planificación de la continuidad de la seguridad de la información
  - A.17.1.2 Implementar la continuidad de la seguridad de la información
  - A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- A.17.2 Redundancias
  - A.17.2.1 Disponibilidad de los recursos de tratamiento de la información

A.18 Cumplimiento
- A.18.1 Cumplimiento de los requisitos legales y contractuales
  - A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
  - A.18.1.2 Derechos de propiedad intelectual (DPI)
  - A.18.1.3 Protección de los registros de la organización
  - A.18.1.4 Protección y privacidad de la información de carácter personal
  - A.18.1.5 Regulación de los controles criptográficos
- 18.2 Revisiones de seguridad de información
  - A.18.2.1 Revisión independiente de la seguridad de la información
  - A.18.2.2 Cumplimiento con las políticas y normas de seguridad
  - A.18.2.3 Comprobación del cumplimiento técnico

2.4 COMPARATIVA ISO/IEC 27001:2005 – ISO/IEC 27001:2013

La implantación de *ISO/IEC 27001:2013* no debería implicar demasiadas complicaciones en una organización que cuente con la versión del 2005 dado que la nueva norma busca simplificar metodologías para lograr una integración más natural en el negocio.

Las diferencias entre la *ISO/IEC 27001:2005* y la *ISO/IEC 27001:2013* se aprecian tanto en la estructura como en los contenidos. Las modificaciones más destacadas las encontramos en el Anexo A, donde el número de dominios ha pasado de 11 a 14 y los controles de 133 a 114.

En la figura 2.7 se esquematizan algunas diferencias entre ambas versiones de la norma para el caso de que estemos considerando una organización que cuente con una certificación previa en *ISO/IEC 27001:2005,* asumiendo que el responsable conoce en profundidad la norma previa.

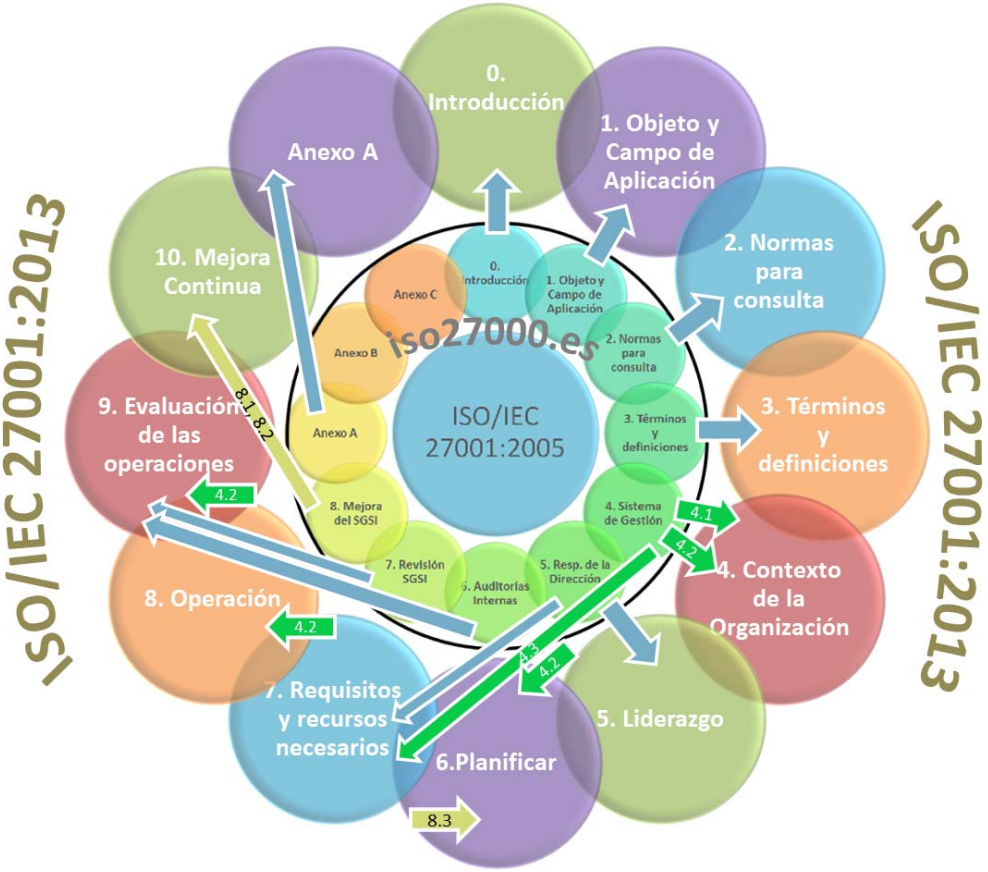

Figura 2.7: Diagrama de relación de la reorganización de la versión 2005 a la 2013.
Fuente: www.iso27000.es

En BSI Group (2013 a; 2013b) encontramos una relación comparativa entre las cláusulas de ambas versiones, que junto con la información del *blog firma-e*, es analizada y detallada a continuación, que se resumen en la tabla 2.2.

Cláusula 0: Introducción

Con grandes similitudes de una versión a otra, cabe destacar que se elimina la definición del proceso PDCA que se encontraba en la sección "Enfoque del proceso". Como se ha mencionado previamente, esta nueva edición requiere de un método que garantice la mejora continua, pero sin obligar a un PDCA en ningún momento. Esta mejora podrá hacerse de forma global mediante cualquier método.

Cláusula 1: Objeto y campo de aplicación

Similar descripción, mientras que antes bastaba con cumplir los requisitos especificados en las cláusulas 4, 5, 6, 7 y 8, ahora es obligatorio cumplir con los requisitos especificados en las cláusulas de la 4 a la 10.

Cláusula 2: Normas para consulta

Se hacía referencia a la norma *ISO/IEC 17799:2005*, ahora la normativa obligatoria de consulta es la *ISO/IEC 27000*.

Cláusula 3: Términos y Definiciones

No encontramos ninguna de las definiciones de términos que encontrábamos en la *ISO/IEC 27001:2005*, todos ellos han sido incluidos en la sección 3 de la ISO/IEC 27000, que es a la que se hace referencia ahora.

Cláusula 4: Sistema de gestión de seguridad de la información

Esta es una de las cláusulas que mayor cambio ha experimentado debido a que en la versión del 2005, el ciclo PDCA se describía en ella por completo. Sin embargo, ahora, no se contempla.

Se menciona el concepto de acción preventiva y establece el contexto para el SGSI indiferentemente del ámbito de la organización. Aparece el nuevo concepto de "Las partes interesadas" como fundamental para definir correctamente el alcance.

Cláusula 5: Responsabilidades de la dirección

En la nueva versión se introduce el concepto de "alta dirección" y se insiste en su compromiso de ser un ejemplo en la gestión del SGSI.

Cláusula 6: Auditorías internas del SGSI y Cláusula 7: Revisión del SGSI por la dirección

Estas dos cláusulas, auditoría interna y revisión por la dirección, se reubican en la nueva norma dentro de las cláusulas 9.2 y 9.3 respectivamente.

Cláusula 8: Mejora del SGSI

La mejora continua y acciones correctivas son en la nueva versión las cláusulas 10.2 y 10.1 respectivamente.

Anexos

El Anexo A normativo ha sido reestructurado y el número de dominios ha pasado de 11 a 14 y los controles de 133 a 114.

Los anexos B y C informativos de la versión del 2005 desaparecen en la versión del 2013 puesto que se la importancia de la seguridad de la información en las organizaciones actuales es un asunto indiscutible.

Tabla 2.2: Mapa de equivalencias entre ISO/IEC 27001:2013 e ISO/IEC 27001:2005
Fuente: BSI group (2013a)

Cláusula en ISO/IEC 27001:2013	Requisito	Equivalencia ISO/IEC 27001:2005
4.1	La organización debe determinar las cuestiones externas e internas…	8.3, 8.3(a), 8.3(e)
4.2(a)	las partes interesadas que son relevantes para el sistema…	5.2.1(c), 7.3(c)(4), 7.3(c)(5)
4.2(b)	los requisitos de estas partes interesadas…	5.2.1(c), 7.3(c)(4), 7.3(c)(5)
4.3	La organización debe determinar los límites y…	4.2.1(a)
4.3(a)	las cuestiones externas e internas referidas en el…	4.2.3(f)
4.3(b)	los requisitos referidos en el ..	4.2.3(f)
4.3(c)	las interfaces y dependencias entre actividades	Requerimiento nuevo
4.3(c)	El alcance debe estar disponible como…	4.3.1(b)
4.4	La organización debe establecer, implementar, mantener…	4.1, 5.2.1(a)
5.1(a)	asegurando que se establecen las política y los objetivos…	4.2.1(b)(3)
5.1(b)	asegurando la integración de los requisitos…	Requerimiento nuevo
5.1(c)	asegurando que los recursos necesarios…	5.1(e)
5.1(d)	comunicando la importancia de una…	5.1(d)
5.1(e)	asegurando que el sistema de gestión de seguridad…	5.1(b), 5.1(g), 5.1(h)
5.1(f)	dirigiendo y apoyando a las personas…	5.1(b), 5.1(g), 5.1(h)
5.1(g)	promoviendo la mejora continua…	5.1(d)
5.1(h)	apoyando otros roles pertinentes de la dirección	5.1
5.2	La alta dirección debe establecer una política…	4.2.1(b)(5), 5.1(a)
5.2(a)	sea adecuada al propósito…	4.2.1(b)
5.2(b)	incluya objetivos de la seguridad de la información…	4.2.1(b)(1)
5.2(c)	incluya el compromiso de cumplir con los requisitos…	4.2.1(b)(2), 4.3.3
5.2(d)	incluya el compromiso de mejora continua…	5.1(d)
5.2(e)	estar disponible como información documentada;	4.3.1(a)
5.2(f)	comunicarse dentro de la organización;	5.1(d)
5.2(g)	estar disponible para las partes interesadas…	4.3.2(f)
5.3	La alta dirección debe asegurarse de que…	5.1(c)

5.3(a)	asegurarse de que el sistema de gestión de la…	4.3.3
5.3(b)	informar a la alta dirección sobre el comportamiento…	4.3.3
6.1.1	Al planificar el sistema de gestión de seguridad…	4.2.1(d), 8.3(a)
6.1.1(a)	asegurar que el sistema de gestión de seguridad…	Requerimiento nuevo
6.1.1(b)	prevenir o reducir efectos indeseados;	Requerimiento nuevo
6.1.1(c)	lograr la mejora continua;	Requerimiento nuevo
6.1.1(d)	las acciones para tratar estos riesgos y …	4.2.1(e)(4), 8.3(b), 8.3(c)
6.1.1(e)(1)	integrar e implementar las acciones en los…	4.3.1(f), 8.3(c)
6.1.1(e)(2)	evaluar la eficacia de estas acciones;	7.2(f)
6.1.2	La organización debe definir y aplicar un proceso…	4.2.1(c), 4.2.1(c)(1)
6.1.2(a)	establezca y mantenga criterios sobre riesgos…	Requerimiento nuevo
6.1.2(a)(1)	los criterios de aceptación de riesgo;	4.2.1(b)(4), 4.2.1(c)(2), 5.1(f)
6.1.2(a)(2)	los criterios para llevar a cabo las apreciaciones…	4.2.3(d)
6.1.2(b)	asegure que las sucesivas apreciaciones de los riesgos…	4.2.1(c)(2)
6.1.2(c)	identifique los riesgos de seguridad de la información.	4.2.1(d)
6.1.2(c)(1)	llevando a cabo el proceso de apreciación de…	4.2.1(d)(1), 4.2.1(d)(2), 4.2.1(d)(3), 4.2.1(d)(4)
6.1.2(c)(2)	identificando a los dueños de los riesgos;	4.2.1(d)(1)
6.1.2(d)	analice los riesgos de seguridad…	4.2.1(e)
6.1.2(d)(1)	valorando las posibles consecuencias que resultarían…	4.2.1(e)(1)
6.1.2(d)(2)	valorando de forma realista la probabilidad…	4.2.1(e)(2)
6.1.2(d)(3)	determinando los niveles de riesgo;	4.2.1(e)(3)
6.1.2(e)	evalúe los riesgos de seguridad de la información:	4.2.1(e)(4)
6.1.2(e)(1)	comparando los resultados del análisis de riesgos…	4.2.1(e)(4)
6.1.2(e)(2)	priorizando el tratamiento de los riesgos…	4.2.1(e)(4)
6.1.2(e)(2)	La organización debe conservar información documentada…	4.3.1(d), 4.3.1(e)
6.1.3	La organización debe definir y efectuar un proceso…	4.2.1(c)(1)

6.1.3(a)	seleccionar las opciones adecuadas de tratamiento de riesgos…	4.2.1(f), 4.2.1(f)(1), 4.2.1(f)(2), 4.2.1(f)(3), 4.2.1(f)(4)
6.1.3(b)	determinar todos los controles que sean necesarios…	4.2.1(g)
6.1.3(c)	comparar los controles determinados en el punto…	4.2.1(j)(1), 4.2.1(j)(3)
6.1.3(d)	elaborar una "Declaración de aplicabilidad"…	4.2.1(j), 4.2.1(j)(1), 4.2.1(j)(2), 4.2.1(j)(3), 4.3.1(i)
6.1.3(e)	formular un plan de tratamiento de riesgos…	4.2.2(a)
6.1.3(f)	obtener la aprobación del plan de tratamiento de…	4.2.1(h)
6.1.3(f)	La organización debe conservar información documentada…	4.3.1(f)
6.2	La organización debe establecer los objetivos…	5.1(b)
6.2(a)	ser coherentes con la política de seguridad..	5.1(d)
6.2(b)	ser medibles (si es posible);	**Requerimiento nuevo**
6.2(c)	tener en cuenta los requisitos de seguridad…	**Requerimiento nuevo**
6.2(c)	y los resultados de la apreciación y del tratamiento…	**Requerimiento nuevo**
6.2(d)	ser comunicados; y	5.1(d)
6.2(e)	ser actualizados, según sea apropiado.	4.2.3(b)
6.2(e)	La organización debe conservar información documentada…	4.3.1(a)
6.2(f)	lo que se va a hacer;	**Requerimiento nuevo**
6.2(g)	qué recursos se requerirán;	**Requerimiento nuevo**
6.2(h)	quién será el responsable;	**Requerimiento nuevo**
6.2(i)	cuándo se finalizará;	**Requerimiento nuevo**
6.2(k)	cómo se evaluarán los resultados.	**Requerimiento nuevo**
7.1	La organización debe determinar y proporcionar….	4.2.2(g), 5.2.1
7.2(a)	determinar la competencia necesaria de las personas…	5.2.2, 5.2.2(a)
7.2(b)	asegurarse de que estas personas sean competentes…	5.2.2
7.2(c)	cuando sea aplicable, poner en marcha acciones…	5.2.2(b), 5.2.2(c)

7.2(d)	conservar la información documentada…	5.2.2(d)
7.3(a)	la política de la seguridad de la….	**Requerimiento nuevo**
7.3(b)	su contribución a la eficacia del sistema de…	4.2.2(e), 5.2.2(d)
7.3(c)	las implicaciones de no cumplir con los requisitos del…	4.2.2(e), 5.2.2(d)
7.4	La organización debe determinar la necesidad de…	4.2.4(c), 5.1(d)
7.4(a)	el contenido de la comunicación;	**Requerimiento nuevo**
7.4(b)	cuando comunicar;	**Requerimiento nuevo**
7.4(c)	a quién comunicar;	**Requerimiento nuevo**
7.4(d)	quien debe comunicar;	**Requerimiento nuevo**
7.4(e)	los procesos por los que debe efectuarse la…	**Requerimiento nuevo**
7.5.1(a)	la información documentada requerida por esta…	4.3.1(a), 4.3.1(b), 4.3.1(h), 4.3.1(i)
7.5.1(b)	la información documentada que la organización …	**Requerimiento nuevo**
7.5.2(a)	la identificación y la descripción…	4.3.2(j)
7.5.2(b)	el formato(por ejemplo, idioma, versión del software…	4.3.1(i)
7.5.2(c)	la revisión y la aprobación con respecto	4.3.2(a), 4.3.2(b)
7.5.3	La información documentada requerida por el sistema…	4.3.2
7.5.3(a)	esté disponible y preparada para su uso…	4.3.2(d)
7.5.3(b)	esté protegida adecuadamente…	4.3.3
7.5.3(c)	distribución, acceso, recuperación y uso;	4.3.2(f), 4.3.2(h), 4.3.2(i)
7.5.3(d)	almacenamiento y preservación , incluida la …	4.3.2(e), 4.3.3
7.5.3(e)	control de cambios (por ejemplo, control de la versión);	4.3.2(c)
7.5.3(f)	retención y disposición.	4.3.2(f)
7.5.3(f)	La información documentada de origen externo…	4.3.2(g)
8.1	La organización debe planificar, implementar….	**Requerimiento nuevo**
8.1	La organización debe implementar también planes…	4.2.2(f)
8.1	En la medida necesaria la organización debe mantener…	4.3.3

8.1	La organización debe controlar los cambios planificados…	A.10.1.2, A.12.5.1, A.12.5.2, A.12.5.3
8.1	revisar las consecuencias de los cambios no previstos…	4.2.2(h), 8.3(b), 8.3(c)
8.1	La organización debe garantizar que los procesos…	A.10.2.1, A.10.2.2, A.10.2.3, A.12.5.5
8.2	La organización debe efectuar apreciaciones…	4.2.3(d)
8.2	La organización debe conservar información documentada…	4.3.1(e)
8.3	La organización debe implementar el plan de tratamiento…	4.2.2(b), 4.2.2(c)
8.3	La organización debe conservar información documentada…	4.3.3
9.1	La organización debe evaluar el desempeño…	4.2.3(a)(3), 4.2.3(b), 4.2.3(c), 4.2.3(f), 6(d)
9.1(a)	a que es necesario hacer seguimiento…	4.2.2(d)
9.1(b)	los métodos de seguimiento, medición….	4.2.2(d)
9.1(c)	cuándo se deben llevar a cabo el seguimiento…	Requerimiento nuevo
9.1(d)	quien debe hacer el seguimiento…	Requerimiento nuevo
9.1(e)	cuando se deben analizar y evaluar los resultados…	4.2.3(b)
9.1(f)	quien debe analizar y evaluar esos resultados.	Requerimiento nuevo
9.1(f)	La organización debe conservar información documentada…	4.3.1(g)
9.2	La organización debe llevar a cabo auditorías internas…	4.2.3(e), 6
9.2(a)(1)	los requisitos propios de la organización…	6(b)
9.2(a)(2)	los requisitos de esta norma internacional.	6(a)
9.2(b)	está implementado y mantenido de manera eficaz.	6(c)
9.2(c)	planificar, establecer, implementar y mantener uno o…	6(d)
9.2(d)	para cada auditoría, definir sus criterios…	6(d)
9.2(e)	seleccionar los auditores y llevar a cabo auditorías para…	6(d)
9.2(f)	asegurarse de que se informa a la dirección…	6(d)
9.2(g)	conservar información documentada…	4.3.1(h), 4.3.3
9.3	La alta dirección debe revisar el sistema de gestión…	5.2.1(e), 7.1
9.3(a)	el estado de las acciones desde anteriores revisiones…	7.2(g)

9.3(b)	los cambios en las cuestiones externas e internas…	4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(4), 4.2.3(d)(5), 4.2.3(d)(6), 7.2(c), 7.2(e), 7.2(h)
9.3(c)	la información sobre el comportamiento de la…	7.2(f)
9.3(c)(1)	no conformidades y acciones correctivas,	7.2(d)
9.3(c)(2)	seguimiento y resultado de las mediciones,	7.2(f)
9.3(c)(3)	resultados de auditoría, y	7.2(a)
9.3(c)(4)	cumplimiento de los objetivos de seguridad de la información.	Requerimiento nuevo
9.3(d)	los comentarios provenientes de las partes…	7.2(b)
9.3(e)	los resultados de la apreciación del riesgo y el estado…	7.2(e), 7.2(f)
9.3(f)	las oportunidades de mejora continua.	7.2(i)
9.3(f)	Los elementos de salida de la revisión por la dirección…	4.2.3(f), 7.1, 7.3(a)
9.3(f)	y cualquier necesidad de cambio en el sistema…	4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(5), 4.2.3(d)(6), 4.2.3(g), 7.1, 7.3(b), 7.3(c), 7.3(c)(1), 7.3(c)(2), 7.3(c)(3), 7.3(c)(4), 7.3(c)(5), 7.3(c) (6), 7.3(d), 7.3€
9.3(f)	La organización debe conservar información documentada…	4.3.1(h), 7.1
10.1(a)	reaccionar ante la no conformidad…	Requerimiento nuevo
10.1(a)(1)	llevar a cabo acciones para controlarla y…	Requerimiento nuevo
10.1(a)(2)	hacer frente a las consecuencias,	Requerimiento nuevo
10.1(b)	evaluar la necesidad de acciones para eliminar…	8.2(c), 8.3(b)
10.1(b)(1)	la revisión de la no conformidad,	8.2(a)

10.1(b)(2)	la determinación de las causas de la no conformidad, y	8.2(b)
10.1(b)(3)	la determinación de si existen no conformidades…	8.3(a)
10.1(c)	implementar cualquier acción necesaria;	4.2.4(b), 8.2, 8.2(d)
10.1(d)	revisar la eficacia de las acciones correctivas…	8.2, 8.2(f)
10.1(e)	si es necesario, hacer cambios al sistema de gestión…	**Requerimiento nuevo**
10.1(e)	Las acciones correctivas deben ser adecuadas…	8.3
10.1(f)	la naturaleza de las no conformidades..	**Requerimiento nuevo**
10.1(g)	los resultados de cualquier acción correctivas.	8.2(e)
10.2	La organización debe mejorar de manera continua…	4.2.4(a), 4.2.4(b), 4.2.4(d), 5.2.1(f), 8.1

CAPÍTULO 3

DISEÑO DEL SISTEMA INTEGRADO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 INTRODUCCIÓN

En este capítulo, se propone una documentación mínima de aplicación en la implantación y mantenimiento del Sistema de seguridad de la información (que aparece resaltada en la Figura 3.1).

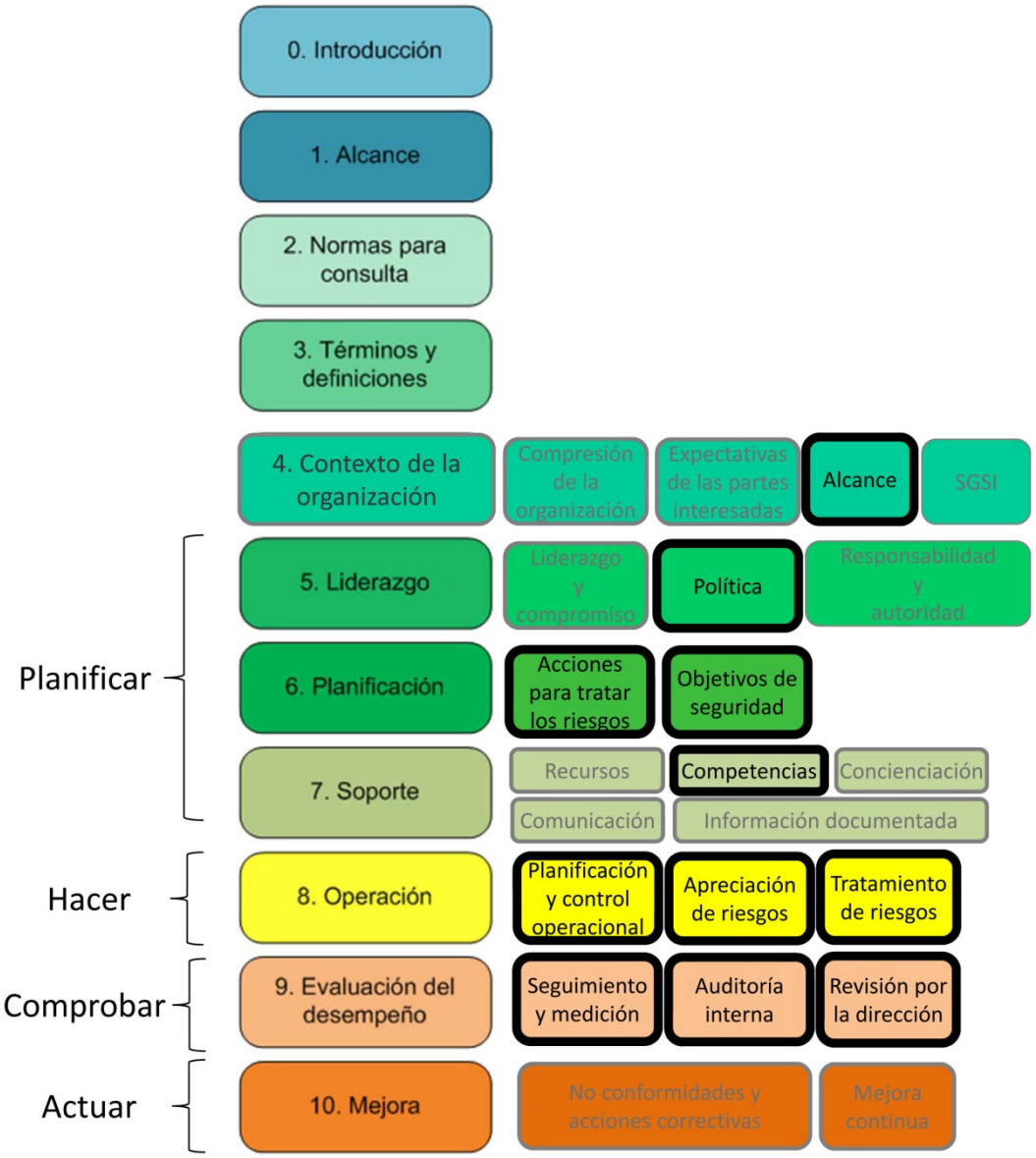

Figura 3.1: Diagrama de la estructura estándar de ISO/IEC 27001:2013 con documentación mínima. Fuente: Elaboración propia

Se propone al menos un modelo de documento por cada uno de los requisitos de ISO/IEC 27001:2013 resaltados en la Figura 3.1 e indicados en la Tabla

3.1 que necesitan obligatoriamente del mantenimiento de una información documentada. La ampliación de esta documentación mínima obligatoria dependerá de las necesidades particulares de la organización.

Tabla 3.1: Relación de clásulas que requieren información documentada (ID)

ISO 27001:2013	ID
Cláusula 0 Introducción	
0.1. Generalidades	
0.2. Compatibilidad con otras normas de sistema de gestión	
Cláusula 1: Objeto y campo de aplicación	
Cláusula 2: Normas para consulta	
Cláusula 3: Términos y Definiciones	
Cláusula 4: Contexto de la Organización	
4.1. Compresión de la organización y de su contexto	
4.2. Compresión de las necesidades y expectativas de las partes interesadas	
4.3. Determinación del alcance del sistema de gestión de seguridad de la información	X
4.4. Sistema de gestión de seguridad de la información	
Cláusula 5: Liderazgo	
5.1. Liderazgo y compromiso	
5.2.Política	X
5.3 Roles, responsabilidades y autoridades en la organización	
Cláusula 6: Planificación	
6.1. Acciones para tratar los riesgos y oportunidades	
6.1.1 Consideraciones generales	
6.1.2 Apreciación de riesgos de seguridad de la información	X
6.1.3 Tratamiento de los riesgos de seguridad de la información	X
6.2. Objetivos de seguridad de la información y planificación para su consecución	X
Cláusula 7: Soporte	
7.1. Recursos	
7.2. Competencia	X
7.3. Concienciación	
7.4. Comunicación	
7.5. Información Documentada	
Cláusula 8: Operación	
8.1. Planificación y control operacional	X
8.2. Apreciación de los riesgos de seguridad de la información	X
8.3. Tratamiento de los riesgos de seguridad de la información	X
Cláusula 9: Evaluación de desempeño	
9.1. Seguimiento, medición, análisis y evaluación	X
9.2. Auditoría interna	X
9.3. Revisión por la dirección	X
Cláusula 10: Mejora	
10.1.No conformidad de acciones correctivas	
10.2. Mejora continua	

3.2 DOCUMENTACIÓN PROPUESTA

Cláusula 4.3 determinación del alcance del sistema de gestión y seguridad de la información

Cada organización debe definir el ámbito de la organización que va a trabajar bajo los requisitos de la norma.

Cláusula 5.2 Política

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DOCUMENTACIÓN PROPUESTA

Desde la Dirección de LA ORGANIZACIÓN existe un interés por asegurar la confidencialidad, integridad, y disponibilidad de los sistemas de información, así como por garantizar la adecuada gestión los servicios de TI prestados a nuestros clientes y velar por el cumplimiento de todas las obligaciones legales aplicables.

Como punto fundamental de la política está la implantación, operación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los estándares internacionales *ISO/IEC 27001:2013*.

Las directrices y objetivos generales relacionados con la Seguridad de la Información y la Gestión de Servicios de TI quedan plasmados en esta Política definida por la Dirección General, forma parte de la política general de la empresa y es consecuente con ella, siendo de aplicación a toda la organización.

Dichas directrices quedan relacionadas a continuación:

- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir todos los requisitos legales aplicables.
- Garantizar servicio ininterrumpido, rápida resolución de incidencias y alta satisfacción del cliente.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Asegurar que todos los empleados conocen sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Gestionar la prestación de los servicios realizados a los clientes de forma eficaz y eficiente, dentro de un ciclo de vida que permita la mejora continua de los procesos implantados.
- Asegurar que los requisitos acordados con los clientes se cumplen y se mantienen

La Dirección dotará al Sistema de Gestión de todas las herramientas precisas, documentalmente establecidas, para asegurar que esta Política es conocida,

comprendida, desarrollada y mantenida al día por todos los niveles de la organización, así como comunicada a todas aquellas personas que trabajan en nombre de LA ORGANIZACIÓN.

Se definirán, como mínimo anualmente, objetivos que serán cuantificables o mensurables siempre que sea posible, para evaluar el grado de consecución de los mismos y establecer las medidas oportunas en el caso de que no se alcancen.

La Dirección del LA ORGANIZACIÓN se compromete a mejorar continuamente la eficacia del Sistema de Gestión.

FECHA
Dirección General
FIRMA DIRECCIÓN

Sub-cláusula 6.1.2 Apreciación de riesgos de seguridad de la información

Sub-cláusula 8.2. Apreciación de los riesgos de seguridad de la información

Apreciación de riesgos de seguridad de la información
DOCUMENTACIÓN PROPUESTA

OBJETO

El presente documento pretende definir una metodología para la realización de una apreciación de riesgos asociados a la seguridad de la información.

ALCANCE

Este procedimiento es de aplicación a toda la información que compone el Sistema de Información de LA ORGANIZACIÓN

DOCUMENTACIÓN DE REFERENCIA

- Norma *ISO/IEC 27001:2013*
- MAGERIT V3, Libro 2: Catálogo de elementos. Editado por el Ministerio de Administraciones Públicas en Madrid, el octubre de 2012. http://publicaciones.administracion.es

ÍNDICE

1. Generalidades

A continuación se detalla la metodología a seguir para realizar las tres partes que componen el análisis de riesgos: inventario de información, análisis de riesgos y gestión de riesgos.

Para el inventario de información, análisis de riesgos y gestión de riesgos se propone emplear el formato ORGANIZACIÓN-AR-XX.

2. Procedimiento

2.1 Identificación de los riesgos de la Seguridad de la Información

Primero se identificará cada riesgo en el formato ORGANIZACIÓN-AR-XX (inventario de información) indicando:

- Nombre del riesgo.
- Dimensión de la seguridad del riesgo. (ver 2.1.1)
- Categoría la información en que se encuentra el riesgo. (ver 2.2.2)
- Dueño del riesgo: Persona o cargo que administra, autoriza el uso, regula o gestiona la información

2.1.1 Asignación del riesgo respondiendo a las tres dimensiones de la seguridad:

- **Confidencialidad** (C): Una pérdida de confidencialidad puede derivar en incidencias de seguridad cuando un usuario no autorizado accede a la información. Este usuario puede adquirir un conocimiento que utilice para perjudicar los intereses de la organización. Se debe valorar la información en función de la importancia que tenga una pérdida de confidencialidad para le organización. Para la valoración de la confidencialidad se emplea la tabla adjunta en el Anexo 1 de este procedimiento.

- **Integridad** (I): Se refiere a la exactitud y completitud de la información. Una pérdida de integridad puede hacernos ver datos que no son correctos o completos. En relación a otras categorías, la pérdida de integridad se refiere a un mal funcionamiento, uso o puesta en marcha indebida. Se debe valorar la información en cuanto a la importancia

que tiene para la organización su integridad. Para la valoración se emplea la tabla adjunta en el anexo 1 de este documento.

- **Disponibilidad** (D): La disponibilidad de una información puede afectar negativamente al negocio, provocando que ciertos procesos se vean mermados o cancelados durante el tiempo que dicho información se encuentra inoperante. Una información disponible debe ser accesible en el momento en el que se necesite. Hay que considerar el tiempo necesario en sustituir y dejar la información como estaba antes de la ocurrencia de algún evento que comprometa su seguridad. Valorar cuanto tiempo podríamos prescindir la información. Para la valoración se emplea la tabla adjunta en el anexo 1 del presente procedimiento.

2.1.2 Clasificación de Categorías la información donde reside la información:

- **Servicios** [S]: Procesos de negocio definidos en el alcance, servicios internos considerados críticos para el funcionamiento de los procesos de negocio. Los servicios de terceros que se consideren importantes también se incluirán.
- **Datos/Información** [D]: Datos de cualquier tipo y formato, independientemente de cómo estén organizados y de dónde estén alojados. Es una información intangible.
- **Instalaciones** [I]: Infraestructura, instalaciones como oficinas, despachos o el CPD.
- **Hardware** [HW]: Considerado como un dispositivo electrónico más la configuración necesaria para que funcione. No se considera la información que tiene, ésta será otro información diferente de la categoría información.
- **Software** [SW]: Aplicaciones informáticas de todo tipo, como ofimática, desarrollo, administración, gestión, de sistemas, etc. Los datos que puedan manejar se considerarán en una información de la categoría información.
- **Soportes de información** [SI]: Dispositivos transportables que poseen información en su interior. También se considera soporte el papel con información impresa.
- **Redes de comunicaciones** [COM]: Red local de la empresa, además de los dispositivos de red, como router, switch, hub, firewall, etc., considerados junto con su configuración.
- **Personal** [P]: Personas concretas que por el conocimiento que poseen, no por la experiencia, se consideran imprescindibles en la empresa.

- **Equipamiento auxiliar** [AUX]: otros equipos que sirven de soporte a los sistemas de información sin estar directamente relacionados con datos.

Por último, para valorar la información deberemos **determinar su Importancia (I)**. Se emplea la siguiente fórmula para su cálculo:

$$I = (D \times I \times C) / 3$$

En función del valor numérico obtenido se asignará un valor de importancia a cada uno de la información según lo indicado en la siguiente tabla:

Valor cualitativo	Valor cuantitativo
Muy alta	Entre 4.5 (no incluido) y 5
Alta	Entre 3.5 (no incluido) y 4.5
Media	Entre 2.5 (no incluido) y 3.5
Baja	Entre 1.5 (no incluido) y 2.5
Muy baja	Entre 1 y 1.5

2.2 Metodología para el análisis de Riesgos

Para determinar el riesgo se deberán seguir los pasos indicados a continuación.

2.2.1. Identificación de las amenazas

Sobre el inventario de información actualizado se determinaran las vulnerabilidades y amenazas asociadas a cada información identificados.

Las amenazas son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en la información. La consecuencia de una amenaza, si se materializa, es un incidente que modifica el estado de la seguridad de la información afectados.

De forma general, se han establecido **4 grupos de amenazas** (basado en el catálogo de MAGERIT). Se pueden consultar en el anexo 2 de este documento:

- Desastres naturales [N].
- De origen industrial [I]
- Ataques intencionados [A]
- Errores y fallos no intencionados [E]

2.2.2 Identificación de las vulnerabilidades

Para cada información se determinarán las vulnerabilidades que podrían hacer que una amenaza se materialice sobre la información correspondiente.

2.2.3 Determinar a qué dimensión de Seguridad afecta la amenaza

Basado en la metodología MAGERIT se indicará a qué dimensión de seguridad afecta cada amenaza. A efectos de análisis de riesgos de seguridad, LA ORGANIZACIÓN identifica estas dimensiones: confidencialidad, integridad y disponibilidad.

Para ello:

- Se indicará 1 si se estima que esa amenaza SI afecta a la dimensión de seguridad.
- Se indicará 0 si se estima que esa amenaza NO afecta a la dimensión de seguridad.

2.2.4 Determinar la probabilidad SIN Salvaguardas

Consiste en la estimación de la probabilidad de ocurrencia de la amenaza sobre la información indicada SIN estar implementadas salvaguardas que puedan reducir o evitar la materialización de la amenaza correspondiente sobre una información.

Se valorará según la propia experiencia de la persona que realiza la valoración, empleando la escala del 1 al 5 indicada en el anexo 1 de este procedimiento.

2.2.5 Determinar el impacto SIN Salvaguardas

Se entiende como impacto el daño causado sobre la empresa, la información y/o sobre una información a consecuencia de la materialización de una amenaza determinada.

Se valorará el impacto de cada amenaza sobre cada información y por cada una de las 3 dimensiones de seguridad establecidas: Confidencialidad, integridad y disponibilidad.

Para la valoración el evaluador empleará su propia experiencia y asignará una puntuación del 1 al 5 según las tablas establecida en el anexo 1 de este documento.

2.2.6 Estimación del Riesgo SIN Salvaguardas

El valor de riesgo de seguridad se obtiene por media aritmética entre el valor de importancia la información, y Probabilidad e impacto en caso de ocurrencia.

Se valora el riesgo de cada amenaza para cada información y para cada dimensión. Es decir:

$$Rs = (V \times Ps \times Is) \times DS$$

En donde:
Rs = Riesgo SIN
V = Importancia de la información
Ps = Probabilidad de ocurrencia de la amenaza para ese información sin haber salvaguardas implementadas
Is= Impacto en caso de ocurrencia sin haber salvaguardas implementadas
DS = Dimensión de Seguridad (confidencialidad, integridad, disponibilidad).

De este modo tendremos 3 riesgos de seguridad por cada información:

- Riesgo para la confidencialidad
- Riesgo para la integridad
- Riesgo para la disponibilidad

Como resultado de la aplicación de la fórmula para el cálculo del riesgo se obtendrá un valor numérico. Cada valor numérico se traduce en un valor "textual" y se codifica según el código de colores mostrados a continuación.

Valor cualitativo		Valor cuantitativo
Muy alto		4-5
Alto		3-3.9
Medio		2-2.99
Bajo		1-1.99
Muy bajo		0-0.99
Sin valor		0

2.2.7 Caracterización de las Salvaguardas

Identificación de las salvaguardas existentes y su estado de implementación. En función del estado de implementación se asignarán unos puntos:

Inexistente = 0
Iniciado = 1
Definido = 2
Gestionado = 3
Optimizado = 4

En función de esta puntuación otorgada y del número de controles implementados se obtendrá un valor de descenso que multiplicará probabilidad e impacto, tal como se describe en el siguiente paso.

El valor de descenso se obtiene por aplicación de la siguiente fórmula:

Descenso (D) = Puntos por implementación de salvaguardas / 4 (puntos totales a obtener)

2.2.8 Evaluación de la probabilidad CON salvaguardas implementadas

Estimación de la probabilidad de ocurrencia tras la implementación de las salvaguardas. Se debe aplicar en este paso el descenso calculado anteriormente.

Se utilizará la fórmula: **Pc = Ps – (Ps x D)**

2.2.9 Evaluación del impacto CON salvaguardas implementadas

Se valorará el impacto de cada amenaza sobre cada información y por cada una de las 3 dimensiones de seguridad establecidas: Confidencialidad,

integridad y disponibilidad, teniendo en cuenta las salvaguardas implementadas.

Se utilizarán las fórmulas:

$$ICc = ICs - (ICs \times D)$$
$$IIc = IIs - (IIs \times D)$$
$$IDc = IDs - (IDs \times D)$$

2.2.10 Evaluación del riesgo CON salvaguardas implementadas

El valor de riesgo de seguridad se obtiene por media aritmética entre el valor de importancia la información, y Probabilidad e impacto en caso de ocurrencia.

Se valora el riesgo de cada amenaza para cada información y para cada dimensión. Es decir:

$$Rc = (V \times Ps \times Is) \times DS$$

En donde:
Rc = Riesgo CON Salvaguardas implementadas
V = Importancia la información
Pc = Probabilidad de ocurrencia de la amenaza para ese información con salvaguardas implementadas
Ic= Impacto en caso de ocurrencia con salvaguardas implementadas
DS = Dimensión de Seguridad (confidencialidad, integridad, disponibilidad).

De este modo tendremos 3 riesgos de seguridad por cada información:

- Riesgo para la confidencialidad
- Riesgo para la integridad
- Riesgo para la disponibilidad

Como resultado de la aplicación de la fórmula para el cálculo del riesgo se obtendrá un valor numérico. Cada valor numérico se traduce en un valor "textual" y se codifica según el código de colores mostrados a continuación.

Valor cualitativo		Valor cuantitativo
Muy alto		4-5
Alto		3-3.9
Medio		2-2.99
Bajo		1-1.99
Muy bajo		0-0.99
Sin valor		0

2.3 Gestión del Riesgo

Una vez realizado el análisis de riesgos, el La Dirección de la Organización debe revisar los resultados obtenidos en función de los cuales, aprobará un nivel de riesgo asumible.

Esta decisión puede verse afectada por modificaciones en la legislación o compromisos con usuarios o proveedores, los

Para aquella información con riesgos asociados por encima del nivel acordado, se establecerá un Plan de Tratamiento de Riesgos, que incluya la definición de controles a implementar, plazos, responsabilidades, los recursos necesarios y descripción de las actividades a realizar.

Como Resumen de las decisiones relativas al tratamiento de riesgos, el comité de seguridad elabora una Declaración de aplicabilidad, que formará parte de la información documentada requerida en la cláusula 6.1.3 Tratamiento de los riesgos de seguridad de la información.

3. Anexos

Anexo 1. Tablas propuestas para el cálculo de importancia y riesgo

Confidencialidad

Valor cualitativo	Valor cuantitativo	Criterio
Muy alta	5	Hacerlo público supone una falta total de confianza y la pérdida de negocio.
Alta	4	Hacerlo público dañaría la imagen y se sufriría una pérdida de confianza.
Media	3	Hacerlo público supone una pérdida leve de confianza de la opinión pública.
Baja	2	Hacerlo público supone una pérdida mínima de confianza de la opinión pública.
Muy baja	1	Se puede hacer público.

Integridad

Valor cualitativo	Valor cuantitativo	Criterio
Muy alta	5	No se puede funcionar sin ello.
Alta	4	Se produce ralentización de actividades y mal funcionamiento del servicio.
Media	3	Se producen errores leves de funcionamiento del servicio.
Baja	2	Se producen errores despreciables que no afectarán prácticamente al servicio
Muy baja	1	No afecta al servicio

Disponibilidad

Valor cualitativo	Valor cuantitativo	Criterio
Muy alta	5	No poder prescindir de la información más de 2 horas.
Alta	4	No poder prescindir de la información más de 1 horas.
Media	3	No poder prescindir de la información más de 1 día.
Baja	2	No poder prescindir de la información más de 2 día.
Muy baja	1	Poder prescindir de la información 2 días o más.

Probabilidad de ocurrencia

Valor cualitativo	Valor cuantitativo	Criterio
Muy alta	5	> 1 vez / mes.
Alta	4	< 1 vez / mes.
Media	3	1 vez / año.
Baja	2	1 vez / 2 años.
Muy baja	1	Improbable que ocurra.

Impacto

Valor cualitativo	Valor cuantitativo	Criterio
Muy alto	5	Daño irrecuperable en alguno de la información de la organización. Paraliza a los servicios prestados por completo Impacto muy grave en otras organizaciones Daño muy grave sobre la imagen de la empresa
Alto	4	Daño recuperable a largo plazo (semanas) en alguno de los información de la organización. Afecta gravemente a los servicios prestados, produciendo interrupción larga (semanas) Impacto grave en otras organizaciones Daño grave sobre la imagen de la empresa
Medio	3	Daño recuperable a medio plazo (días) en alguno de los información de la organización. Afecta a los servicios prestados, produciendo interrupción de los mismos durante medio plazo de tiempo (días) Impacto leve en otras organizaciones Daño leve sobre la imagen de la empresa.
Baja	2	Daño recuperable a corto plazo (horas) en alguno de los información de la organización. Afecta a los servicios prestados, produciendo interrupción de los mismos durante un corto periodo de tiempo (horas) Sin impacto en otras organizaciones Sin daño sobre la imagen de la empresa.
Muy Baja	1	Daño irrelevante en alguna información de la organización. No afecta operativamente a los servicios prestados Sin impacto en otras organizaciones Sin daño sobre la imagen de la empresa.

Anexo 2. Propuesta de catálogo de amenazas

A continuación se muestra un catálogo de amenazas y un catálogo de evaluación para ayudar a realizar el análisis y evaluación de riesgos según la metodología MAGERIT (versión 3). Para cada amenaza se muestra un cuadro como este:

Catálogo de amenazas	
[N] Desastres Naturales	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
[I] De origen industrial	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres Industriales
	[I.3] Contaminación mecánica
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura y/o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios y suministros esenciales
	[I.10] Degradación de los soportes de almacenamiento de la información
	[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.3] Errores de monitorización (log)
	[E.4] Errores de configuración
	[E.7] Deficiencias en la organización
	[E.8] Difusión de software dañino
	[E.9] Errores de re-encarnamiento
	[E.10] Errores de secuencia
	[E.14] Escapes de información
	[E.15] Alteración de la información
	[E.16] Introducción de información incorrecta
	[E.17] Degradación de la información
	[E.18] Destrucción de la información
	[E.19] Divulgación de la información

	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento/actualización de programas
	[E.23] Errores de mantenimiento/actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.28] Indisponibilidad del personal
[A] Ataques intencionados	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.9] Re-encarnamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[A.12] Análisis de tráfico
	[A.13] Repudio
	[A.14] Intercepción de información (escucha)
	[A.15] Modificación de la información
	[A.16] Introducción de falsa información
	[A.17] Corrupción de la información
	[A.18] Destrucción de la información
	[A.19] Divulgación de la información
	[A.22] Manipulación de programas
	[A.24] Denegación de servicio
	[A.25] Robo
	[A.26] Ataque destructivo
	[A.27] Ocupación enemiga
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social

Catálogo de evaluación:

[Código] Descripción sucinta de lo que puede pasar	
Tipos de información: - Que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** - De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: Complementaria o más detallada de la amenaza: lo que le puede ocurrir a la información del tipo indicado con las consecuencias indicadas	

Sub-cláusula 6.1.3 Tratamiento de los riesgos de seguridad de la información y Sub-cláusula 8.3. Tratamiento de los riesgos de seguridad de la información

".

RUPO	ID	CONTROL	PREGUNTA	R.	COMENT.
5. Política de Seguridad	5.1 Directrices de gestión de la seguridad de la información				
	5.1.1	Políticas para la seguridad de la información	¿Existe un documento de política de seguridad disponible para todos los usuarios?		
	5.1.1	Políticas para la seguridad de la información	¿Se han tenido en consideración en su elaboración los riesgos a los que está expuesta la organización?		
	5.1.1	Políticas para la seguridad de la información	¿Se ha comunicado el documento de forma que sea entendible y accesible a los destinatarios?		
	5.1.1	Políticas para la seguridad de la información	¿Se han definido indicadores de eficacia de la política de seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Queda establecido en el documento el compromiso de la dirección con la seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Incluye el documento una definición de seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Y una definición de las responsabilidades en materia de gestión de la seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Y el alcance de la seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Y la importancia de la seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Y el establecimiento de la meta de la dirección?		
	5.1.1	Políticas para la seguridad de la información	¿Y una explicación de las políticas, principios y normas más importantes?		
	5.1.1	Políticas para la seguridad de la	¿Y una definición de los objetivos globales de la		

		información	seguridad?		
	5.1.1	Políticas para la seguridad de la información	¿Y referencias a la documentación que sustenta la política de seguridad?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Se han programado revisiones periódicas de la efectividad de la política?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Y del coste de los controles?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Y del impacto de los controles en el trabajo diario?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Y del efecto de los cambios tecnológicos?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Se ha designado un responsable del mantenimiento y revisión de la política de seguridad?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Se hacen revisiones regulares de la política de seguridad?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Se ha tenido en cuenta que el proceso de revisión responda a los cambios en la valoración del riesgo?		
	5.1.2	Revisión de las políticas para la seguridad de la información	¿Existe un procedimiento que especifique el proceso de revisión?		
seguridad	**6.1 Organización Interna.**				

	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas las responsabilidades para proteger y controlar la información y los sistemas?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Se han identificado los activos y los procesos de seguridad asociados con cada sistema?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Se ha designado al responsable de cada activo o proceso de seguridad?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidos y documentados los niveles de autorización?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están documentados los detalles de esa responsabilidad?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Se ha designado al responsable para ejecutar los procesos?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas y documentadas todas las responsabilidades para proteger los activos?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas y documentadas todas actividades específicas relacionadas con la seguridad?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas y documentadas las funciones y responsabilidades de los puestos de trabajo?		
	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas y documentadas las responsabilidades para implantar la política de seguridad?		

	6.1.1	Roles y responsabilidades en seguridad de la información	¿Están definidas y documentadas las responsabilidades para mantener esta política?		
	6.1.2	Segregación de tareas	¿Cuenta el sistema con protección frente a cambios en los tipos de mensajes y eventos que se registran?		
	6.1.2	Segregación de tareas	¿Y a la edición o destrucción de los logs?		
	6.1.2	Segregación de tareas	¿Y a que se exceda la capacidad de almacenamiento del sistema donde se almacenan los logs?		
	6.1.2	Segregación de tareas	¿Se tienen en cuenta los requerimientos legales para los registros que pueden ser utilizados como evidencias?		
	6.1.2	Segregación de tareas	¿Existen controles para garantizar que una persona no pueda acceder, modificar o utilizar activos sin que exista una autorización previa, o al menos un conocimiento por parte del propietario del activo?		
	6.1.2	Segregación de tareas	¿Están separados los procesos de solicitud de los de aprobación?		
	6.1.2	Segregación de tareas	¿Se prevé la segregación de tareas en el diseño de los controles de seguridad?		
	6.1.2	Segregación de tareas	¿Se suplen las necesidades de segregación con controles de monitorización cuando no es posible segregar?		
	6.1.2	Segregación de tareas	¿Se mantiene la independencia de la auditoria de seguridad?		

	6.1.2	Segregación de tareas	¿Están segregadas las tareas, para reducir la oportunidad de o malos usos de los sistemas?		
	6.1.2	Segregación de tareas	¿Están protegidos tanto los logs como las herramientas que los generan?		
	6.1.3	Contacto con las autoridades	¿Existen procedimientos que contengan cómo y cuándo se contacta con los organismos públicos (bomberos, cuerpos de seguridad, servicios de emergencia) y el reporte de incidentes de seguridad?		
	6.1.3	Contacto con las autoridades	¿Mantiene su empresa contactos con organismos públicos (bomberos, cuerpos de seguridad, servicios de emergencia?		
	6.1.3	Contacto con las autoridades	Cuando la organización es atacada por Internet. ¿Se tiene en cuenta la necesidad que un externo (proveedores de servicios de Internet u operadores de telecomunicaciones) tome medidas contra la fuente de ataque?		
	6.1.4	Contacto con grupos de interés especial	¿Mantiene su empresa contactos con organizaciones, foros, comités especialistas de seguridad?		
	6.1.4	Contacto con grupos de interés especial	¿Estos contactos permiten compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas y vulnerabilidades?		
	6.1.4	Contacto con grupos de interés especial	¿Estos contactos aseguran la compresión de la seguridad de la información de forma		

			actualizada y completa?		
	6.1.5	Seguridad de la información en la gestión de proyectos	¿La seguridad de la información es tratada dentro de la gestión de proyectos?		
	6.1.5	Seguridad de la información en la gestión de proyectos	¿La seguridad de la información es tratada como un proyecto?		
	6.2 Los dispositivos móviles y el teletrabajo				
	6.2.1	Política de dispositivos móviles	¿Están dotados de sistemas de protección antivirus?		
	6.2.1	Política de dispositivos móviles	¿Se les ha impartido una formación especial a los usuarios de estos equipos en materia de seguridad?		
	6.2.1	Política de dispositivos móviles	¿Se dispone de un seguro para estos equipos?		
	6.2.1	Política de dispositivos móviles	¿Se protegen físicamente los equipos frente a robos?		
	6.2.1	Política de dispositivos móviles	¿Se actualizan adecuadamente las herramientas de protección contra código malicioso?		
	6.2.1	Política de dispositivos móviles	¿Se requiere a los usuarios que prevengan el que otras personas puedan ver la información contenida en los sistemas?		
	6.2.1	Política de dispositivos móviles	¿Y para la conexión a redes?		
	6.2.1	Política de dispositivos móviles	¿Se adoptan medidas especiales de seguridad para el uso de redes inalámbricas?		

	6.2.1	Política de dispositivos móviles	¿Se adoptan medidas especiales de seguridad para el uso de ordenadores portátiles?		
	6.2.1	Política de dispositivos móviles	¿Y de uso de criptografía?		
	6.2.1	Política de dispositivos móviles	¿Y de control de accesos?		
	6.2.1	Política de dispositivos móviles	¿Define la política los requerimientos de seguridad física?		
	6.2.1	Política de dispositivos móviles	¿Y de teléfonos móviles?		
	6.2.1	Política de dispositivos móviles	¿Y de tarjetas inteligentes?		
	6.2.1	Política de dispositivos móviles	¿Y de PDAs?		
	6.2.1	Política de dispositivos móviles	¿Y de copias de seguridad?		
	6.2.1	Política de dispositivos móviles	¿Y para el uso de estos sistemas en lugares públicos?		
	6.2.1	Política de dispositivos móviles	¿Existe una política y los controles para la protección contra el riesgo de trabajar con portátiles y comunicaciones móviles?		
	6.2.2	Teletrabajo	¿A la finalización del teletrabajo se retiran los derechos de acceso?		
	6.2.2	Teletrabajo	¿Y se solicita la devolución del equipamiento?		
	6.2.2	Teletrabajo	¿Se audita y monitoriza la seguridad del teletrabajo?		
	6.2.2	Teletrabajo	¿Se cuenta con procedimientos para copias de seguridad y continuidad de las operaciones?		

	6.2.2	Teletrabajo	¿Se ha contratado un seguro que cubra el hardware, software e información?		
	6.2.2	Teletrabajo	¿Se proporciona el soporte y mantenimiento necesario para hardware y software?		
	6.2.2	Teletrabajo	¿Y de seguridad física?		
	6.2.2	Teletrabajo	¿Y mobiliario?		
	6.2.2	Teletrabajo	¿Se dan guías sobre cómo gestionar el acceso de familiares o amigos?		
	6.2.2	Teletrabajo	¿Existen políticas y procedimientos para autorizar y controlar las actividades de tele trabajo?		
	6.2.2	Teletrabajo	¿Y comunicaciones?		
	6.2.2	Teletrabajo	¿Se proporciona un equipo informático adecuado para el teletrabajo?		
	6.2.2	Teletrabajo	¿Existe un proceso formal para autorizar el teletrabajo?		
7. Seguridad relativa a los recursos humanos	7.1 Antes del empleo				
	7.1.1	Investigación de antecedentes	¿Se estudia la credibilidad de los empleados que acceden a información sensible?		
	7.1.1	Investigación de antecedentes	¿Están incluidas en el contrato con las agencias de contratación sus responsabilidades en el proceso de selección?		
	7.1.1	Investigación de antecedentes	¿Se confirman las titulaciones académicas?		
	7.1.1	Investigación de antecedentes	¿Se comprueban las referencias aportadas en el CV?		
	7.1.1	Investigación de antecedentes	¿Se verifica que son ciertos los datos del CV cuando se solicita un		

			puesto de trabajo?		
	7.1.1	Investigación de antecedentes	¿Y las certificaciones profesionales?		
	7.1.1	Investigación de antecedentes	¿Se comprueba la identidad del candidato mediante DNI, pasaporte u otro documento?		
	7.1.2	Términos y condiciones del empleo	¿Continua esa responsabilidad durante un tiempo tras la finalización del contrato?		
	7.1.2	Términos y condiciones del empleo	¿Se incluye cómo actuar en caso de que el empleado no cumpla con los requisitos de seguridad?		
	7.1.2	Términos y condiciones del empleo	¿Y las responsabilidades y obligaciones legales (LOPD, LSSI, LPI, etc.)?		
	7.1.2	Términos y condiciones del empleo	¿Establece que las responsabilidades se extienden más allá del ámbito de la organización y el horario laboral?		
	7.1.2	Términos y condiciones del empleo	¿Están establecidas las responsabilidades de los empleados, relativas a la seguridad, en los términos y condiciones del contrato de trabajo?		
	7.2 Durante el empleo				
	7.2.1	Responsabilidades de gestión	¿Conoce la dirección los problemas personales de los empleados en puestos especialmente críticos que puedan afectar a su trabajo?		
	7.2.1	Responsabilidades de gestión	¿Garantiza la dirección que los empleados, usuarios subcontratados y terceras partes cumplen con las políticas y normas		

			establecidas?		
	7.2.1	Responsabilidades de gestión	¿Firman todas las partes la recepción y conocimiento de normas, políticas, etc. antes de iniciar su función laboral en la empresa?		
	7.2.1	Responsabilidades de gestión	¿Se mantienen actualizadas y correctamente distribuidas las normas, procedimientos, política, etc. a todos los empleados?		
	7.2.1	Responsabilidades de gestión	¿Se revisan y aprueban periódicamente los procedimientos del personal por empleados de más categoría?		
	7.2.1	Responsabilidades de gestión	¿Y los problemas financieros?		
	7.2.1	Responsabilidades de gestión	¿Y los cambios de comportamiento?		
	7.2.1	Responsabilidades de gestión	¿Y los cambios de estilo de vida?		
	7.2.1	Responsabilidades de gestión	¿Y las ausencias recurrentes del puesto de trabajo?		
	7.2.1	Responsabilidades de gestión	¿Y las posibles situaciones de depresión?		
	7.2.1	Responsabilidades de gestión	¿Y las situaciones de stress?		
	7.2.1	Responsabilidades de gestión	¿Se revisa periódicamente el trabajo de todo el personal?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y para los freelance, estudiantes en prácticas, becarios o contratados a tiempo parcial?		

	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y para los consultores externos?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Se imparte esta formación antes de que se les dé acceso a los sistemas?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Se imparten periódicamente las actualizaciones necesarias de la formación?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Se incluye en la formación los requerimientos de seguridad?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y las responsabilidades legales?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y el uso correcto de los sistemas?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y para los servicios de limpieza, cafetería o vigilancia?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Y el uso correcto de las aplicaciones?		
	7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Reciben los empleados y usuarios de terceras partes la formación apropiada, relativa a políticas y procedimientos de seguridad?		

	7.2.3	Proceso disciplinario	¿Se notifica periódicamente las consecuencias de infringir las normas de seguridad como recordatorio?		
	7.2.3	Proceso disciplinario	¿Existe un proceso disciplinario para tratar las violaciones de las políticas y procedimientos de seguridad?		
	7.2.3	Proceso disciplinario	¿Lo conocen todos los empleados?		
	7.3 Finalización del empleo o cambio en el puesto de trabajo				
	7.3.1	Responsabilidades ante la finalización o cambio	¿Están definidas las responsabilidades de todas las partes implicadas en la finalización o cambios en los contratos y puestos de trabajo?		
	7.3.1	Responsabilidades ante la finalización o cambio	¿Se han incluido estas responsabilidades en los contratos laborales?		
	7.3.1	Responsabilidades ante la finalización o cambio	¿Y en los contratos con terceros y subcontratados?		
8 Gestión de Activos	**8.1 Responsabilidad sobre los activos**				
	8.1.1	Inventario de Activos	¿Y su situación habitual?		
	8.1.1	Inventario de Activos	¿Se incluye en el inventario la clasificación de seguridad de los activos?		
	8.1.1	Inventario de Activos	¿Y los relacionados con el sistema informático, como servidores, PCs, portátiles, faxes, routers, switches, discos, cintas, licencias de software, software del sistema, herramientas y utilidades de desarrollo, etc.?		
	8.1.1	Inventario de Activos	¿Y la pertenencia de los activos?		

	8.1.1	Inventario de Activos	¿Se han incluido en el inventario los activos de entorno, como suministro de energía o de comunicaciones, unidades de aire acondicionado, personal, muebles, etc.?		
	8.1.1	Inventario de Activos	¿Y los que son información, como ficheros, bases de datos, documentación del sistema, manuales de los usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, etc.?		
	8.1.1	Inventario de Activos	¿Y los relativos a servicios, como correo, web, ERP, CRM, Intranet, etc.?		
	8.1.1	Inventario de Activos	¿Y los de tipo general, como imagen de la organización, confianza de clientes, etc.?		
	8.1.1	Inventario de Activos	¿Existe un inventario actualizado de los activos del sistema de información?		
	8.1.2	Propiedad de los activos	¿Es actualizado cuando las circunstancias lo requieren?		
	8.1.2	Propiedad de los activos	¿Se ha identificado nominalmente la propiedad de los activos del sistema de información?		
	8.1.2	Propiedad de los activos	¿Se han designado otras responsabilidades con respecto a los activos, p.e. los depositarios, los administradores, etc.?		
	8.1.2	Propiedad de los activos	¿Están formalmente previstas las revisiones de la propiedad de los activos?		

	8.1.3	Uso aceptable de los activos	¿Se incluye las normas de uso correcto en los contratos establecidos con todas las partes?		
	8.1.3	Uso aceptable de los activos	¿Conocen todas las partes (internas y externas) que interactúan con los activos las normas establecidas?		
	8.1.3	Uso aceptable de los activos	¿Están documentadas formalmente los usos apropiados que deben darse a los activos del sistema de información?		
	8.1.4	Devolución de activos	¿Se actualiza el inventario de activos?		
	8.1.4	Devolución de activos	¿Esta formalizado el proceso de devolución de activos tras la finalización de la relación laboral?		
	8.1.4	Devolución de activos	En caso de terceras partes o activos personales de los empleados (portátiles, agendas, etc.), ¿se garantiza la devolución de los activos procesados por estos?		
	8.2 Clasificación de la información				
	8.2.1	Clasificación de la información	¿Se han previsto las situaciones que hacen que cambie la clasificación de la información?		
	8.2.1	Clasificación de la información	¿Se cataloga la información en relación con su criticidad (en términos de confidencialidad o integridad)?		
	8.2.1	Clasificación de la información	¿Se revisa periódicamente la clasificación de la información?		

	8.2.1	Clasificación de la información	¿Existe un esquema para clasificar la información y los sistemas en función de su confidencialidad o importancia?		
	8.2.1	Clasificación de la información	¿Se cataloga la información en relación con su valor o importancia para la organización?		
	8.2.2	Etiquetado de la información	¿Se marca la información crítica o sensible de salida de los sistemas?		
	8.2.2	Etiquetado de la información	¿Existe un procedimiento para la copia de la información?		
	8.2.2	Etiquetado de la información	¿Y en los soportes de almacenamiento?		
	8.2.2	Etiquetado de la información	¿Existen procedimientos para identificar y usar la información, según su clasificación?		
	8.2.2	Etiquetado de la información	¿Y en las transferencias de ficheros?		
	8.2.2	Etiquetado de la información	¿Y en los correos electrónicos?		
	8.2.2	Etiquetado de la información	¿Y para el almacenamiento?		
	8.2.2	Etiquetado de la información	¿Y para la transmisión por correo ordinario, correo electrónico y fax?		
	8.2.2	Etiquetado de la información	¿Y para la transmisión oral?		
	8.2.2	Etiquetado de la información	¿Y para la destrucción?		
	8.2.2	Etiquetado de la información	¿Se marca la clasificación en los informes impresos?		
	8.2.2	Etiquetado de la información	¿Y en las pantallas de salida?		
	8.2.2	Etiquetado de la información	¿Se marca electrónicamente la información que no se puede marcar físicamente?		

	8.2.3	Manipulado de la información	¿Se mantienen listas de usuarios autorizados para acceder a la información sensible?		
	8.2.3	Procedimiento de tratamiento de la información	¿Se auditan periódicamente los permisos de acceso a la información?		
	8.2.3	Procedimiento de tratamiento de la información	¿Se etiqueta toda la información?		
	8.2.3	Procedimiento de tratamiento de la información	¿Sea aplica el principio de distribuir el mínimo posible?		
	8.2.3	Procedimiento de tratamiento de la información	¿Se asegura que la entrada, el proceso y la salida de la información son correctas?		
	8.2.3	Procedimiento de tratamiento de la información	¿Se han establecido restricciones de acceso para evitar accesos no autorizados?		
	8.2.3	Procedimiento de tratamiento de la información	¿Se tiene en cuenta la clasificación de la información para aplicar un método de manipular y almacenar apropiado?		
	8.2.3	Procedimiento de tratamiento de la información	¿Existen procedimientos para manejar y almacenar la información, que la protejan de malos usos?		
	8.2.3	Procedimiento de tratamiento de la información	¿Están protegidos los spool de datos de acuerdo con la clasificación de la información?		
	8.3 Manipulación de los soportes				
	8.3.1	Gestión de soportes extraíbles	¿Existen entornos seguros para almacenar los soportes de acuerdo a las especificaciones del fabricante?		
	8.3.1	Gestión de soportes extraíbles	¿Se han previsto medidas especiales para la información con un periodo de retención superior a la vida media		

			del soporte donde está almacenada?		
	8.3.1	Gestión de soportes extraíbles	¿Se clasifican todos los soportes de información de acuerdo a la política de clasificación?		
	8.3.1	Gestión de soportes extraíbles	¿Se permiten grabadoras y dispositivos que permitan grabar soportes removibles solo en aquellos casos en que esté justificada la necesidad?		
	8.3.1	Gestión de soportes extraíbles	¿Se controla y registra la E/S de estos soportes?		
	8.3.1	Gestión de soportes extraíbles	¿Están documentados los procedimientos y niveles de autorización para la gestión de soportes?		
	8.3.1	Gestión de soportes extraíbles	¿Se borran de forma segura cuando ya no se necesitan?		
	8.3.1	Gestión de soportes extraíbles	¿Hay procedimientos para gestionar soportes removibles con información como discos, CDs, informes impresos,...?		
	8.3.2	Eliminación de soportes	¿Tienen procedimientos para asegurar la destrucción de los soportes que ya no son necesarios?		
	8.3.2	Eliminación de soportes	¿Se tiene en cuenta la clasificación de la información para aplicar un método de destrucción apropiado?		

	8.3.2	Eliminación de soportes	¿Disponen de lugares para almacenar de forma segura los soportes que van a ser destruidos hasta que llegue el momento de la destrucción?		
	8.3.2	Eliminación de soportes	¿Tiene procedimientos para identificar los soportes que deben destruirse de forma segura?		
	8.3.2	Eliminación de soportes	¿Cuentan con herramientas de destrucción de documentación?		
	8.3.2	Eliminación de soportes	En caso de que tenga subcontratada la destrucción de soportes, ¿Verifica periódicamente la fiabilidad de la empresa?		
	8.3.2	Eliminación de soportes	¿Se ha tenido en cuenta el riesgo de agregación de información no sensible?		
	8.3.2	Eliminación de soportes	¿Se han contemplado cláusulas de confidencialidad para su destrucción?		
	8.3.2	Eliminación de soportes	¿Se registra la destrucción de soportes de información?		
	8.3.3	Soportes físicos en tránsito	¿Se toma alguna medida especial con los soportes en tránsito con información sensible?		
	8.3.3	Soportes físicos en tránsito	¿Existen procedimiento de identificación de mensajeros o transportistas autorizados?		
	8.3.3	Soportes físicos en tránsito	¿Se han definido procedimientos para identificar a los mensajeros autorizados?		

	8.3.3	Soportes físicos en tránsito	¿Se utilizan valijas o contenedores especiales en algún caso?		
	8.3.3	Soportes físicos en tránsito	¿Se utilizan envases con detección de intento de apertura?		
	8.3.3	Soportes físicos en tránsito	¿Se utiliza fraccionamiento de envíos en algún caso?		
	8.3.3	Soportes físicos en tránsito	¿Se utilizan controles criptográficos en formatos lógicos?		
9. Control de acceso	**9.1 Requisitos de negocio para el control de acceso**				
	9.1.1	Política de control de acceso	¿Se han definido perfiles de control de acceso para los roles más frecuentes en la organización?		
	9.1.1	Política de control de acceso	¿Se han estudiado conjuntamente los controles de acceso físico y lógico?		
	9.1.1	Política de control de acceso	¿Se ha establecido un criterio de "todo está prohibido, salvo lo que está expresamente autorizado?		
	9.1.1	Política de control de acceso	¿Existe un procedimiento para la retirada de los derechos de acceso a un usuario?		
	9.1.1	Política de control de acceso	¿Existe un procedimiento para la revisión periódica del control de accesos?		
	9.1.1	Política de control de acceso	¿Se han definido los requerimientos para la autorización formal de las solicitudes de acceso?		
	9.1.1	Política de control de acceso	¿Se ha previsto una segregación de las tareas relacionadas con el control de accesos, como la solicitud, autorización y administración?		
	9.1.1	Política de control de acceso	¿Y los requisitos legales?		

	9.1.1	Política de control de acceso	¿Y la coherencia entre el control de accesos y el esquema de clasificación de la información?		
	9.1.1	Política de control de acceso	¿Se ha desarrollado una política de control de accesos?		
	9.1.1	Política de control de acceso	¿Tiene en cuenta la política de control de accesos los requisitos de seguridad de las distintas aplicaciones de negocio?		
	9.1.1	Política de control de acceso	¿Se han definido las reglas y los derechos de acceso para cada grupo o categoría de usuarios?		
	9.1.1	Política de control de acceso	¿Y el principio de necesidad de saber?		
	9.1.1	Política de control de acceso	¿Y los compromisos contractuales?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Se ha verificado que la política de uso de los servicios de red sea coherente con la política de control de accesos?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Y los motivos para acceder a la red y a los servicios?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Está garantizado que los usuarios sólo pueden acceder a los servicios para los que tienen autorización?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Se ha desarrollado una política que especifique el uso de la red y de sus servicios?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Especifica la política las redes y servicios a los que está permitido acceder?		
	9.1.2	Acceso a las redes y a los servicios de red	¿Y los controles y procedimientos para proteger el acceso a la red?		

	9.1.2	Acceso a las redes y a los servicios de red	¿Y el procedimiento de autorización de acceso?		
	9.2 Gestión de acceso de usuario				
	9.2.1	Registro y baja de usuario	¿Se verifica que los derechos de acceso sean adecuados?		
	9.2.1	Registro y baja de usuario	¿Se verifica periódicamente que no existan cuentas con identificadores de usuario redundantes?		
	9.2.1	Registro y baja de usuario	¿Se mantiene una relación de los niveles de autorización de los usuarios?		
	9.2.1	Registro y baja de usuario	¿Se les solicita que firmen un acuse de recibo indicando que han entendido sus derechos de acceso?		
	9.2.1	Registro y baja de usuario	¿Se revisan periódicamente los registros de acceso de los usuarios?		
	9.2.1	Registro y baja de usuario	¿Se verifica que el usuario tenga derecho a acceder a la información o sistema?		
	9.2.1	Registro y baja de usuario	¿Tienen todos los usuarios un identificador único?		
	9.2.1	Registro y baja de usuario	¿Quedan registrados los accesos de los usuarios a los servicios y sistemas?		
	9.2.1	Registro y baja de usuario	¿Tiene cada usuario un identificador único?		
	9.2.1	Registro y baja de usuario	¿Se impide la inclusión de características del usuario o niveles de privilegio en su identificador, p.e. administrador, backup, director, etc.?		

	9.2.1	Registro y baja de usuario	¿Se han implementado métodos de identificación avanzada para dispositivos críticos, p.e. tarjetas criptográficas, tokens, biométricos, etc.?		
	9.2.1	Registro y baja de usuario	¿Se autoriza formalmente el uso de identificadores compartidos?		
	9.2.2	Provisión de acceso a usuario	¿Se cancelan todos los derechos de los usuarios que cambian de función, o trabajo, o abandonan la organización?		
	9.2.2	Provisión de acceso a usuario	¿Se garantiza que los usuarios no podrán acceder al sistema o a la información hasta que el proceso de autorización se haya completado?		
	9.2.3	Gestión de privilegios de acceso	¿Y un registro de todos los privilegios concedidos?		
	9.2.3	Gestión de privilegios de acceso	¿Está controlada la gestión de privilegios?		
	9.2.3	Gestión de privilegios de acceso	¿Se propicia el desarrollo de rutinas o aplicaciones especiales que reduzcan la necesidad de asignar privilegios especiales?		
	9.2.3	Gestión de privilegios de acceso	¿Se asignan los privilegios especiales a un identificador de usuario diferente al que ese usuario emplea habitualmente?		
	9.2.3	Gestión de privilegios de acceso	¿Están identificados los privilegios especiales de acceso de cada aplicación o sistema?		
	9.2.3	Gestión de privilegios de acceso	¿Se asignan los privilegios caso a caso y evento a evento?		

	9.2.3	Gestión de privilegios de acceso	¿Existe un procedimiento de autorización para la concesión de privilegios?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Existe un canal seguro para notificar las contraseñas de los usuarios?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Se modifican las password por defecto de las aplicaciones y sistemas comerciales?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Se almacenan las contraseñas en lugar seguro?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Son distintas para cada usuario los password temporales?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Se verifica la identidad de los usuarios cuando solicitan passwords nuevas o cambios?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Se asigna una contraseña de acceso inicial para su posterior cambio personal del usuario?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Firman los empleados un compromiso de mantener la confidencialidad de sus passwords?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	¿Existe un proceso para la gestión de passwords?		
	9.2.4	Gestión de la información secreta de autenticación de usuarios	Se solicita a los usuarios un acuse de recibo de los password?		
	9.2.5	Revisión de derechos de acceso de usuario	¿Se mantiene un registro de las modificaciones de los privilegios?		
	9.2.5	Revisión de derechos de acceso de usuario	¿Y tras los cambios de personal?		

	9.2.5	Revisión de derechos de acceso de usuario	¿Se revisan periódicamente los derechos de acceso, por ejemplo cada 6 meses?		
	9.2.5	Revisión de derechos de acceso de usuario	¿Se revisan con una frecuencia menor (por ejemplo cada 3 meses) las autorizaciones de acceso con privilegios especiales?		
	9.2.6	Retirada o reasignación de los derechos de acceso	¿Está formalizado el proceso de retirada de los derechos de acceso de los empleados, subcontratados y terceras partes que finalizan los contratos?		
	9.2.6	Retirada o reasignación de los derechos de acceso	¿Y de los derechos de acceso físico?		
	9.3 Responsabilidades de usuario				
	9.3.1	Uso de la información secreta de autenticación	¿Se establece un procedimiento para asegurar que se cambien periódicamente?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que contengan cifras y letras?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que no sean vulnerables a un ataque por diccionario?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que sean fáciles de recordar y difíciles de adivinar?		
	9.3.1	Uso de la información secreta de autenticación	¿Y sobre la longitud mínima de las contraseñas?		
	9.3.1	Uso de la información secreta de autenticación	¿Y que las cambien siempre que tengan la constancia o sospecha de que alguien la conoce?		
	9.3.1	Uso de la información secreta de autenticación	¿Y que no las almacenen de ninguna forma que no haya sido aprobada explícitamente?		

	9.3.1	Uso de la información secreta de autenticación	¿Se les solicita a los usuarios que mantengan en secreto sus contraseñas?		
	9.3.1	Uso de la información secreta de autenticación	¿Se indica a los usuarios que sigan buenas prácticas en la selección y uso de passwords?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que no utilicen ningún sistema de login automático que recuerde las claves?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que utilicen claves diferentes para asuntos de trabajo y asuntos personales?		
	9.3.1	Uso de la información secreta de autenticación	¿Y de que no reutilicen las contraseñas?		
	9.4 Control de acceso a sistemas y aplicaciones				
	9.4.1	Restricción del acceso a la información	¿Se controlan los derechos de acceso (lectura, escritura, control total, etc.)?		
	9.4.1	Restricción del acceso a la información	¿Está restringido el acceso a la información y aplicaciones de negocio?		
	9.4.1	Restricción del acceso a la información	¿Se controlan los derechos de acceso de otras aplicaciones?		
	9.4.1	Restricción del acceso a la información	¿Se asegura que los datos de salida de las funciones son los mínimos necesarios?		
	9.4.1	Restricción del acceso a la información	¿Se modifican los menús de las aplicaciones para que los usuarios solo puedan acceder a las funciones de las aplicaciones a las que están autorizados?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y qué desconecte el enlace tras un número determinado de intentos fallidos?		

	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que introduzca un retardo tras cada intento fallido de log on?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y qué oculte los caracteres del password que se introduce?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que muestre información de cualquier intento fallido tras el último satisfactorio?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que determine el tiempo máximo para completar el proceso de log on?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que bloquee la cuenta tras un número determinado de intentos fallidos?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que no transmita el password en claro a través de la red?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que limite el número de intentos fallidos de log on?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que en caso de fallo, no indique que campo es el que no es correcto?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y qué valide los datos solo cuando se hayan introducido todos?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que no se disponga de ayudas que puedan dar pistas a los usuarios no autorizados?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y muestra una leyenda indicando que solo deben acceder usuarios autorizados?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se ha tenido en cuenta que el proceso de log on no de ninguna información del sistema o aplicación hasta que se haya finalizado el proceso?		

	9.4.2	Procedimientos seguros de inicio de sesión	¿Se exige un log on seguro para acceder al sistema operativo?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que cuando se haga un log on satisfactorio se muestre la fecha y hora del último log on satisfactorio?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Y que registre todos los intentos de login, satisfactorios o no?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se determina el tiempo de espera en base al nivel de riesgo?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se cierra la aplicación y la sesión de red tras un tiempo superior de inactividad?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se limpian las pantallas tras un tiempo de inactividad?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se cortan las sesiones que están inactivas durante un periodo determinado de tiempo?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se han definido ventanas horarias para las conexiones?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Existen restricciones en las horas a las que se pueden realizar conexiones a aplicaciones de alto riesgo, así como en su duración?		
	9.4.2	Procedimientos seguros de inicio de sesión	¿Se solicita a los usuarios que vuelvan a autenticarse tras un periodo de tiempo?		
	9.4.3	Sistema de gestión de contraseñas	¿Previene la reutilización de passwords?		
	9.4.3	Sistema de gestión de contraseñas	¿Transmite las claves cifradas o hasheadas?		
	9.4.3	Sistema de gestión de contraseñas	¿Almacena las claves cifradas o hasheadas?		

	9.4.3	Sistema de gestión de contraseñas	¿Almacena las passwords en ficheros distintos de los datos de aplicación?		
	9.4.3	Sistema de gestión de contraseñas	¿Oculta en pantalla los caracteres de las passwords cuando se teclean?		
	9.4.3	Sistema de gestión de contraseñas	¿Y el cambio de password en el primer log on?		
	9.4.3	Sistema de gestión de contraseñas	¿Y el cambio periódico de passwords?		
	9.4.3	Sistema de gestión de contraseñas	¿Fuerza el uso de passwords de calidad?		
	9.4.3	Sistema de gestión de contraseñas	¿Permite a los usuarios seleccionar y cambiar sus passwords?		
	9.4.3	Sistema de gestión de contraseñas	¿Fuerza el uso de Ids y passwords individuales?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Están documentados los niveles de autorización?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Están restringidos y controlados los programas de utilidades del sistema?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Se han desarrollado procedimientos de identificación, autenticación y autorización para el uso de las utilidades de sistema?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Están segregadas las utilidades de sistemas del software de las aplicaciones?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Se autoriza el uso de utilidades caso a caso y para situaciones concretas?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Se mantiene el número de usuarios con acceso a las utilidades del sistema limitado al mínimo posible?		

	9.4.4	Uso de utilidades con privilegios del sistema	¿Se mantiene un registro de los usos de utilidades del sistema?		
	9.4.4	Uso de utilidades con privilegios del sistema	¿Están deshabilitadas todas las utilidades que no sean necesarias?		
	9.4.5	Control de acceso al código fuente de los programas	¿Está separado e inaccesible para otras áreas de actividad?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se mantienen las librerías en un entorno seguro?		
	9.4.5	Control de acceso al código fuente de los programas	¿Está controlado el acceso a las librerías de los programas fuente?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se autoriza formalmente la actualización de librerías de programas fuente y la entrega de programas fuente a los programadores?		
	9.4.5	Control de acceso al código fuente de los programas	¿Existe un procedimiento establecido para gestión del código fuente del programa y de las librerías de programa fuente?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se registra el acceso a las fuentes por parte de los usuarios?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se auditan periódicamente?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se mantiene adecuadamente un control de cambios y versiones?		
	9.4.5	Control de acceso al código fuente de los programas	¿Existe un proceso basado en la necesidad de saber para autorizar acceso a las fuentes?		
	9.4.5	Control de acceso al código fuente de los programas	¿Se establecen propietarios de los códigos fuente?		
Cripto	**10.1 Controles criptográficos**				

	10.1.1	Política de uso de los controles criptográficos	¿Existe una autorización previa al personal autorizado al uso de estas herramientas?		
	10.1.1	Política de uso de los controles criptográficos	¿Existe una política de uso de controles de cifrado para la protección de la información?		
	10.1.1	Política de uso de los controles criptográficos	¿Se aplica la firma digital o los códigos de autenticación de mensajes para proteger la autenticidad e integridad de la información?		
	10.1.1	Política de uso de los controles criptográficos	Si se utilizan servicios de terceros, ¿se contempla en el contrato este control?		
	10.1.1	Política de uso de los controles criptográficos	¿Se bloquea la entrada de este tipo de datos a las redes de la organización?		
	10.1.1	Política de uso de los controles criptográficos	¿Se informa a todos los usuarios de los peligros de instalar certificados digitales de sitios de internet de dudosa confianza?		
	10.1.1	Política de uso de los controles criptográficos	¿Y en los sistemas públicos cuando es necesario almacenar información sensible?		
	10.1.1	Política de uso de los controles criptográficos	¿Se cifran los datos almacenados en sistemas multiusuario?		
	10.1.1	Política de uso de los controles criptográficos	¿Se elimina la copia de los datos en claro una vez que se han cifrado?		
	10.1.1	Política de uso de los controles criptográficos	¿Se ha realizado una evaluación de riesgos para determinar el nivel de protección que debería recibir la información, el tipo de medida, con qué propósito y en qué procesos de negocio?		

	10.1.1	Política de uso de los controles criptográficos	¿Se aplica el cifrado para proteger la confidencialidad de la información crítica o sensible?		
	10.1.1	Política de uso de los controles criptográficos	¿Existen normas para determinar cuándo se debe usar criptografía?		
	10.1.1	Política de uso de los controles criptográficos	¿Se forma a los usuarios de controles criptográficos?		
	10.1.1	Política de uso de los controles criptográficos	¿Se han definido responsabilidades de la implantación de la política y de la gestión de claves?		
	10.1.1	Política de uso de los controles criptográficos	¿Se gestionan las claves de forma adecuada?		
	10.1.1	Política de uso de los controles criptográficos	¿Se han considerado herramientas criptográficas para protección de información sensible transportada en soportes de datos o soportes móviles, dispositivos o a través de líneas de comunicación?		
	10.1.1	Política de uso de los controles criptográficos	¿Existe un proceso de autorización previa para el uso de firma digital?		
	10.1.1	Política de uso de los controles criptográficos	¿Existe un procedimiento de recuperación de datos cifrados ante un desastre?		
	10.1.2	Gestión de las claves	¿Se protegen las claves de los usuarios para evitar el uso fraudulento?		
	10.1.2	Gestión de las claves	¿Se han establecido los procedimientos de recuperación de claves ante una solicitud legal o un proceso judicial?		

	10.1.2	Gestión de las claves	¿Permiten estos sistemas la solicitud, generación, descarga y revocación automatizada de claves a disposición de los usuarios formalmente autorizados?		
	10.1.2	Gestión de las claves	¿Están localizados en un entorno seguro los sistemas de gestión de claves?		
	10.1.2	Gestión de las claves	¿Existe un procedimiento formal de recuperación del sistema de gestión de claves?		
	10.1.2	Gestión de las claves	¿Existe un responsable encargado de la gestión de las claves criptográficas?		
	10.1.2	Gestión de las claves	¿Se revisa periódicamente el correcto funcionamiento de las aplicaciones de gestión, así como de la validez y caducidad de las claves?		
11. Seguridad física y del entorno	**11.1 Áreas Seguras**				
	11.1.1	Perímetro de seguridad física	¿Existe un perímetro de seguridad para proteger las áreas donde están los sistemas?		
	11.1.1	Perímetro de seguridad física	¿Existen barreras físicas (paredes, puertas, vallas, etc.) que lo delimiten?		
	11.1.1	Perímetro de seguridad física	¿La solidez de las barreras es proporcional a la importancia de los activos?		
	11.1.1	Perímetro de seguridad física	¿Se cuenta con un sistema de control de acceso físico?		
	11.1.1	Perímetro de seguridad física	¿Llegan las barreras desde el suelo real al techo real?		

	11.1.1	Perímetro de seguridad física	¿Tienen todas las puertas antiincendios alarma y cierre automático?		
	11.1.2	Controles físicos de entrada	¿Se revisan periódicamente los derechos de acceso a las áreas seguras?		
	11.1.2	Controles físicos de entrada	¿Se exige a toda persona que esté en las áreas seguras que lleven un elemento identificativo claramente visible?		
	11.1.2	Controles físicos de entrada	¿Están las áreas de seguridad protegidas por controles de entrada, para permitir el acceso sólo al personal autorizado?		
	11.1.2	Controles físicos de entrada	¿Se les informa a los visitantes de las medidas de seguridad y procedimientos de emergencia?		
	11.1.2	Controles físicos de entrada	¿Se registran las horas de entrada y salida de todas las visitas?		
	11.1.2	Controles físicos de entrada	¿Se autentica de alguna forma la identidad del personal que accede a las zonas seguras?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Se han instalado sistemas de detección de intrusos que cubran todas las ventanas y puertas?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Se guardan copias de seguridad de toda la información en un lugar seguro fuera de las instalaciones?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Existe un área especial donde se almacene el material inflamable o peligroso?		

	11.1.3	Seguridad de oficinas, despachos y recursos	¿Están protegidos las oficinas y despachos que tienen algún requerimiento de seguridad especial?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Están separados los sistemas propios de los gestionados por terceros?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Se mantienen cerradas puertas y ventanas cuando no hay nadie?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Existe un área de seguridad donde se localicen fotocopiadoras, faxes, etc.?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Se evitan señales o letreros que permitan identificar las zonas seguras?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Se sitúan los sistemas críticos siempre fuera de las zonas accesibles al público?		
	11.1.3	Seguridad de oficinas, despachos y recursos	¿Está restringido el acceso a listados de teléfonos internos o a los directorios?		
	11.1.4	Protección contra las amenazas externas y ambientales	¿Se han considerado las amenazas del entorno en la definición de los requerimientos de seguridad física de la organización (tormentas, terremotos, incendios, y otras catástrofes naturales)?		
	11.1.4	Protección contra las amenazas externas y ambientales	¿Y las amenazas procedentes de las organizaciones cercanas por su actividad o características de negocio?		
	11.1.5	El trabajo en áreas seguras	¿Existen controles físicos especiales para trabajar en las áreas de		

			seguridad?		
	11.1.5	El trabajo en áreas seguras	¿Se controla el acceso de cámaras fotográficas u otros mecanismos de filmación?		
	11.1.5	El trabajo en áreas seguras	¿Se cuida que sólo las personas que lo necesitan para realizar su trabajo conozcan las áreas seguras y lo que se hace en ellas?		
	11.1.5	El trabajo en áreas seguras	¿Se mantienen las áreas seguras siempre cerradas?		
	11.1.6	Áreas de carga y descarga	¿Están las áreas de entradas y salidas de mercancías aisladas del área de sistemas?		
	11.1.6	Áreas de carga y descarga	¿Existe un registro de acceso a las zonas de carga y descarga de mercancías?		
	11.1.6	Áreas de carga y descarga	¿Existen controles que impidan el acceso no autorizado desde estas áreas al resto de dependencias?		
	11.1.6	Áreas de carga y descarga	¿Se inspecciona el material decepcionado antes de introducirlo en las dependencias?		
	11.1.6	Áreas de carga y descarga	¿Se registra el material recibido a través de estas áreas?		
	11.2 Seguridad de los equipos				
	11.2.1	Emplazamiento y protección de equipos	¿Están los equipos situados o protegidos para reducir las situaciones de riesgo o de acceso no autorizado?		
	11.2.1	Emplazamiento y protección de equipos	¿Se sitúan los equipos para minimizar el riesgo de robo, incendio, inundación, etc.?		

	11.2.1	Emplazamiento y protección de equipos	¿Se ha contemplado la posibilidad de daños por incidentes ajenos, p.e. incendendio o inundaciones en edificios vecinos?		
	11.2.1	Emplazamiento y protección de equipos	¿Se vigilan las condiciones medioambientales, entiéndase AC, calefacción, humos etc.?		
	11.2.1	Emplazamiento y protección de equipos	¿Prohíbe la política de seguridad fumar, beber, comer, etc., cerca de los sistemas?		
	11.2.1	Emplazamiento y protección de equipos	¿Se tienen precauciones para prevenir la visión de información en las pantallas?		
	11.2.2	Instalaciones de suministro	¿Existen dispositivos que permitan evacuación de emergencia en dependencias con cerraduras eléctricas en caso de necesidad?		
	11.2.2	Instalaciones de suministro	¿Existe medios para el apagado ordenado de los dispositivos?		
	11.2.2	Instalaciones de suministro	¿Existen redes redundantes de suministro eléctrico?		
	11.2.2	Instalaciones de suministro	¿Existen contratos que garanticen el suministro de combustible?		
	11.2.2	Instalaciones de suministro	¿Y dispositivos que permitan un apagado urgente y ordenado en caso de emergencia?		
	11.2.2	Instalaciones de suministro	¿Existen pararrayos?		
	11.2.2	Instalaciones de suministro	¿Están protegidos los equipos contra fallos de corriente, climatización, suministros de agua, etc.?		
	11.2.2	Instalaciones de suministro	¿Existen generadores de respaldo?		

	11.2.3	Seguridad de cableado	¿Y de inundaciones?		
	11.2.3	Seguridad de cableado	¿Existen protecciones en los puntos de conexión a la red de comunicaciones?		
	11.2.3	Seguridad de cableado	¿Se utilizan canalizaciones seguras o blindadas para el cableado de comunicaciones?		
	11.2.3	Seguridad de cableado	¿Existen detectores de incendio bajo falso suelo o falso techo?		
	11.2.3	Seguridad de cableado	¿Están aislados el cableado de suministro eléctrico del de comunicaciones?		
	11.2.3	Seguridad de cableado	¿Se oculta bajo falso suelo o techo?		
	11.2.3	Seguridad de cableado	¿Están protegidos contra daños o escuchas los cables que transmitan datos o soporten servicios de información?		
	11.2.3	Seguridad de cableado	¿Se utiliza cableado de fibra óptica?		
	11.2.4	Mantenimiento de los equipos	¿Se mantienen los equipos en base a las recomendaciones del fabricante y/o procedimientos documentados?		
	11.2.4	Mantenimiento de los equipos	¿Se realizan revisiones periódicas de mantenimiento?		
	11.2.4	Mantenimiento de los equipos	¿Existe autorización previa para realizar tareas de mantenimiento?		
	11.2.4	Mantenimiento de los equipos	¿Se mantiene registro de las acciones de mantenimiento?		

	11.2.4	Mantenimiento de los equipos	¿Se realizan tareas de protección cuando los equipos salen de la organización por tareas de mantenimiento, p.e. retirar el HD?		
	11.2.5	Retirada de materiales propiedad de la empresa	¿Se necesita una autorización para sacar de las oficinas equipos, información o software?		
	11.2.5	Retirada de materiales propiedad de la empresa	¿Se registra la salida de material fuera de la organización?		
	11.2.5	Retirada de materiales propiedad de la empresa	¿Se mantiene actualizado el inventario de activos?		
	11.2.5	Retirada de materiales propiedad de la empresa	¿Se avisa a los usuarios de incidentes relacionados con la sustracción de equipos?		
	11.2.5	Retirada de materiales propiedad de la empresa	¿Existen seguros que cubran sustracciones en la organización?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Se necesita autorización previa para extraer sistemas de información fuera de las dependencias de la organización?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Existen seguros que cubran incidentes en estos equipos?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Se mantiene registro de las acciones de mantenimiento?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Contempla la política de seguridad como usar los equipos fuera de la organización, p.e. equipos desatendidos?		

	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Existen procedimientos de seguridad y que cubran la seguridad de los sistemas cuando se usan fuera de las instalaciones de la empresa?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Y controles especiales en los desplazamientos?		
	11.2.6	Seguridad de los equipos fuera de las instalaciones	¿Están estos dispositivos sujetos a tareas de mantenimiento?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Existen dispositivos ignífugos para guardar información sensible?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Existe una política de uso de impresoras y fotocopiadoras?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Tienen las fotocopiadoras dispositivos de control de acceso?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Disponen los dispositivos sistemas de desconexión o bloqueo automático de sesiones?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Se mantiene la información bajo llave cuándo no se está utilizando?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Existe una política de pantallas y mesas limpias para los entornos de trabajo?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Existen políticas que impidan la reutilización de dispositivos de almacenamiento con información sensible?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Se utilizan técnicas avanzadas de eliminación de información de dispositivos con información sensible?		
	11.2.7	Reutilización o eliminación segura	¿Se borra la información de los equipos antes de		

		de equipos	reutilizarlos?		
	11.2.7	Reutilización o eliminación segura de equipos	¿Están controlados los puntos de salida y entrada del correo, fax o similares?		
	11.2.8	Equipo de usuario desatendido	¿Se cierran las sesiones de trabajo o se bloquean los equipos de forma automática?		
	11.2.8	Equipo de usuario desatendido	¿Existen mecanismos físicos que impidan acceso a los equipos?		
	11.2.8	Equipo de usuario desatendido	¿Se solicita a los usuarios adoptar medidas de protección con los equipos desatendidos?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Existe una política de pantallas y mesas limpias?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Están controlados los puntos de salida y entrada del correo, fax o similares?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Disponen los dispositivos sistemas de desconexión o bloqueo automático de sesiones?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Se solicita que se retiren de las fotocopiadoras, faxes, etc. los documentos con información sensible?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Se han previsto controles para limitar el uso de las fotocopiadoras?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿La política tiene en cuenta el esquema de clasificación de la información?		
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	¿Se mantiene la información bajo llave cuándo no se está utilizando?		
d de las	**12.1 Procedimientos y responsabilidades operacionales**				

12.1.1	Documentación de los procedimientos de operación	¿Se incluyen instrucciones para manejar los errores o situaciones de excepción que puedan darse durante la ejecución del procedimiento?		
12.1.1	Documentación de los procedimientos de operación	¿Y los cambios en la configuración de los sistemas?		
12.1.1	Documentación de los procedimientos de operación	¿Y la identificación del terminal?		
12.1.1	Documentación de los procedimientos de operación	¿Están documentados y mantenidos los procedimientos operacionales?		
12.1.1	Documentación de los procedimientos de operación	¿Incluyen los logs del control de accesos el ID de usuario?		
12.1.1	Documentación de los procedimientos de operación	¿Se mantienen registros de auditoria del control de accesos?		
12.1.1	Documentación de los procedimientos de operación	¿Se especifica la forma de gestionar los registros de auditoria?		
12.1.1	Documentación de los procedimientos de operación	¿Y el uso de privilegios especiales?		
12.1.1	Documentación de los procedimientos de operación	¿Están detallados los datos de contacto de las personas de soporte?		
12.1.1	Documentación de los procedimientos de operación	¿Y la aceptación o denegación de intentos de acceso a datos o recursos?		
12.1.1	Documentación de los procedimientos de operación	¿Se detallan los tiempos de inicio y final de cada proceso?		
12.1.1	Documentación de los procedimientos de operación	¿Y para las copias de respaldo?		
12.1.1	Documentación de los procedimientos de operación	¿Se incluyen en los procedimientos de cada proceso instrucciones para la gestión de la información relacionada		

		con el proceso?		
12.1.1	Documentación de los procedimientos de operación	¿Incluyen información detallada de los pasos a ejecutar en cada proceso?		
12.1.1	Documentación de los procedimientos de operación	¿Aprueba la dirección estos documentos?		
12.1.1	Documentación de los procedimientos de operación	¿Se trata de documentos formalizados?		
12.1.1	Documentación de los procedimientos de operación	¿Están especificados los pasos para el arranque, reinicio y apagado de los sistemas?		
12.1.1	Documentación de los procedimientos de operación	¿Y las direcciones de red de origen y destino?		
12.1.1	Documentación de los procedimientos de operación	¿Y los protocolos utilizados?		
12.1.1	Documentación de los procedimientos de operación	¿Y las alarmas generadas por el sistema de control de accesos?		
12.1.1	Documentación de los procedimientos de operación	¿Y las activaciones y desactivaciones de las herramientas de seguridad, como antivirus o firewalls?		
12.1.1	Documentación de los procedimientos de operación	¿Y los archivos a los que se ha accedido?		
12.1.1	Documentación de los procedimientos de operación	¿Y la fecha y hora de eventos importantes como log on o log off?		
12.1.2	Gestión de cambios	¿Se identifican y registran los cambios significativos?		
12.1.2	Gestión de cambios	¿Y a desactivaciones no autorizadas?		
12.1.2	Gestión de cambios	¿Y a las interconexiones de los sistemas afectados?		

12.1.2	Gestión de cambios	¿Y a experiencias anteriores?		
12.1.2	Gestión de cambios	¿Y al valor o criticidad de la información procesada?		
12.1.2	Gestión de cambios	¿Se establece la periodicidad de la revisión de los resultados de la monitorización en base a la criticidad de las aplicaciones o procesos?		
12.1.2	Gestión de cambios	¿Y los cambios, o intentos de cambio, en los controles de seguridad y su configuración?		
12.1.2	Gestión de cambios	¿Y los intentos de acceso no autorizados?		
12.1.2	Gestión de cambios	¿Y los privilegios con los que se llevan a cabo las operaciones?		
12.1.2	Gestión de cambios	¿Se monitoriza que los accesos a datos y sistemas sean los autorizados?		
12.1.2	Gestión de cambios	¿Existe un control de cambios formal para los sistemas y aplicaciones?		
12.1.2	Gestión de cambios	¿Se planifican y prueban los cambios antes de pasarlos a producción?		
12.1.2	Gestión de cambios	¿Se hace un análisis del impacto potencial de los cambios?		
12.1.2	Gestión de cambios	¿Cuenta con un procedimiento para comunicar los cambios a las personas afectadas?		
12.1.2	Gestión de cambios	¿Se genera un registro de auditoria de cada cambio con toda la información relevante?		
12.1.2	Gestión de cambios	¿Se han establecido procedimientos para la monitorización del uso de los sistemas de información?		

12.1.2	Gestión de cambios	¿Existe un proceso formal de aprobación de los cambios propuestos?		
12.1.2	Gestión de cambios	¿Se ha decidido lo que hay que monitorizar y con qué nivel apoyándose en el análisis de riesgos?		
12.1.2	Gestión de cambios	¿Dispone de procedimientos de marcha atrás en caso de fallo para abortar y y recuperar el cambio?		
12.1.3	Gestión de capacidades	¿Cuenta el sistema con protección frente a cambios en los tipos de mensajes y eventos que se registran?		
12.1.3	Gestión de capacidades	¿Y a la edición o destrucción de los logs?		
12.1.3	Gestión de capacidades	¿Y a que se exceda la capacidad de almacenamiento del sistema donde se almacenan los logs?		
12.1.3	Gestión de capacidades	¿Se tienen en cuenta los requerimientos legales para los registros que pueden ser utilizados como evidencias?		
12.1.3	Gestión de capacidades	¿Existen controles para garantizar que una persona no pueda acceder, modificar o utilizar activos sin que exista una autorización previa, o al menos un conocimiento por parte del propietario del activo?		
12.1.3	Gestión de capacidades	¿Están separados los procesos de solicitud de los de aprobación?		
12.1.3	Gestión de capacidades	¿Se prevé la segregación de tareas en el diseño de los controles de seguridad?		

12.1.3	Gestión de capacidades	¿Se suplen las necesidades de segregación con controles de monitorización cuando no es posible segregar?		
12.1.3	Gestión de capacidades	¿Se mantiene la independencia de la auditoria de seguridad?		
12.1.3	Gestión de capacidades	¿Están segregadas las tareas, para reducir la oportunidad de o malos usos de los sistemas?		
12.1.3	Gestión de capacidades	¿Están protegidos tanto los logs como las herramientas que los generan?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se revisan periódicamente los logs de los administradores?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se ha analizado el nivel de separación requerido por la organización?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Está limitado el acceso a las herramientas de desarrollo desde el entorno de producción?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Existen perfiles distintos para cada usuario en los entornos de prueba y producción?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Y el proceso o aplicación involucrado?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Están separados los entornos de desarrollo, pruebas y producción?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Y el tipo de fallo?		

12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Y el tipo de evento?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se registra la fecha y hora del evento?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se mantiene un log de las actividades del administrador del sistema?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se muestran mensajes que le informen al usuario si está trabajando el entorno de pruebas o en el de producción?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Y el administrador involucrado?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se garantiza que no se copia información sensible al entorno de pruebas?		
12.1.4	Separación de los recursos de desarrollo, prueba y operación	¿Se han definido los controles para transferir aplicaciones desde desarrollo a operación?		
12.2 Protección contra el software malicioso (malware)				
12.2.1	Controles contra el código malicioso	¿Se dispone de una política que proteja a la organización de los riesgos de obtener ficheros y software de redes externas?		
12.2.1	Controles contra el código malicioso	¿Y para la notificación y recuperación frente a ataques por código malicioso?		
12.2.1	Controles contra el código malicioso	¿Y para la formación en el uso de las herramientas relacionadas?		

12.2.1	Controles contra el código malicioso	¿Están definidas las responsabilidades para tratar la protección de sistemas frente a código malicioso?		
12.2.1	Controles contra el código malicioso	¿Se realiza un chequeo antivirus para la navegación Web?		
12.2.1	Controles contra el código malicioso	¿Se chequea en más de un punto la entrada de ficheros adjuntos a los correos electrónicos y las descargas de internet?		
12.2.1	Controles contra el código malicioso	¿Se cuenta con una herramienta para la detección y corrección de código malicioso instalada en todos los ordenadores para analizar cualquier archivo que se vaya a introducir en el ordenador a través de soportes electrónicos u ópticos, o a través de la red		
12.2.1	Controles contra el código malicioso	¿Se revisa regularmente el software y los datos contenidos en los sistemas que soporten servicios críticos para el negocio?		
12.2.1	Controles contra el código malicioso	¿Se dispone de una política que prohíba el uso de software no autorizado?		
12.2.1	Controles contra el código malicioso	¿Existen procedimientos implantados para proteger a la empresa contra software malicioso?		
12.2.1	Controles contra el código malicioso	¿Se dispone de copias de respaldo de aplicaciones y datos para recuperarse de un ataque por código malicioso?		

12.2.1	Controles contra el código malicioso	¿Se mantienen los responsables actualizados sobre las noticias o nuevos eventos relacionados con código malicioso?		
12.2.1	Controles contra el código malicioso	¿Se investiga formalmente la existencia de software o datos desautorizados o no aprobados?		
12.2.1	Controles contra el código malicioso	¿Se ha previsto alguna forma de diferenciar entre hoaxes y código malicioso?		
12.2.1	Controles contra el código malicioso	¿Se cuenta con los planes de continuidad de negocio adecuados para recuperarse ante un ataque por código malicioso?		
12.2.1	Controles contra el código malicioso	¿Cuenta la organización con controles que aseguren que el código móvil autorizado está funcionando de acuerdo con la política de seguridad?		
12.2.1	Controles contra el código malicioso	¿Se ha previsto la ejecución de código móvil solo en entorno aislados lógicamente?		
12.2.1	Controles contra el código malicioso	¿Y el bloqueo de cualquier uso de código móvil?		
12.2.1	Controles contra el código malicioso	¿Y el bloqueo de la recepción de código móvil?		
12.2.1	Controles contra el código malicioso	¿Y el control de los recursos disponibles a los que pueda acceder el código móvil?		
12.2.1	Controles contra el código malicioso	¿Y la aplicación de controles criptográficos para autenticar el código móvil?		

12.3 Copias de seguridad				
12.3.1	Copias de seguridad de la información	¿Se verifican periódicamente las copias de seguridad?		
12.3.1	Copias de seguridad de la información	¿Están especificados los periodos de retención de las copias de seguridad de acuerdo con las necesidades de negocio y los requerimientos legales?		
12.3.1	Copias de seguridad de la información	¿Se han previsto medidas para proteger físicamente los soportes donde se almacenan las copias de seguridad?		
12.3.1	Copias de seguridad de la información	¿Se hace copia de seguridad de todo (programas, configuraciones y datos) lo necesario para restaurar los servicios críticos?		
12.3.1	Copias de seguridad de la información	¿Se aplican técnicas de cifrado para proteger las copias de seguridad cuando existen requerimientos de confidencialidad especiales?		
12.3.1	Copias de seguridad de la información	¿Se verifican periódicamente los procedimientos de restauración?		
12.3.1	Copias de seguridad de la información	¿Se almacenan las copias de seguridad en un emplazamiento suficientemente alejado del principal como para no verse afectado si se produce un desastre?		
12.3.1	Copias de seguridad de la información	¿Están documentados los procedimientos de restauración?		
12.3.1	Copias de seguridad de la información	¿Se ha especificado de qué y con qué frecuencia hay que hacer copias de		

		seguridad?		
12.3.1	Copias de seguridad de la información	¿Se hacen regularmente copias de seguridad?		
12.3.1	Copias de seguridad de la información	¿Se comprueba periódicamente que los tiempos de restauración de las copias previstos en los procedimientos coinciden con los reales?		
12.4 Registros y supervisión				
12.4.1	Registro de eventos	¿Se revisan las alarmas generadas por el sistema de control de accesos?		
12.4.1	Registro de eventos	¿Se revisan los protocolos utilizados?		
12.4.1	Registro de eventos	¿Se revisan las direcciones de red de origen y destino?		
12.4.1	Registro de eventos	¿Se revisan los archivos a los que se ha accedido?		
12.4.1	Registro de eventos	¿Se revisan la identificación del terminal?		
12.4.1	Registro de eventos	¿Se revisan las activaciones y desactivaciones de las herramientas de seguridad, como antivirus o firewalls?		
12.4.1	Registro de eventos	¿Se revisan los cambios en la configuración de los sistemas?		
12.4.1	Registro de eventos	¿Se revisan la aceptación o denegación de intentos de acceso a datos o recursos?		
12.4.1	Registro de eventos	¿Se mantienen registros de auditoria del control de accesos?		
12.4.1	Registro de eventos	¿Incluyen los logs del control de accesos el ID de usuario?		

12.4.1	Registro de eventos	¿Y la fecha y hora de eventos importantes como log on o log off?		
12.4.1	Registro de eventos	¿Y el uso de privilegios especiales?		
12.4.1	Registro de eventos	¿Se establece la periodicidad de la revisión de los resultados de la monitorización en base a la criticidad de las aplicaciones o procesos?		
12.4.1	Registro de eventos	¿Y los privilegios con los que se llevan a cabo las operaciones?		
12.4.1	Registro de eventos	¿Y los cambios, o intentos de cambio, en los controles de seguridad y su configuración?		
12.4.1	Registro de eventos	¿Y los intentos de acceso no autorizados?		
12.4.1	Registro de eventos	¿Y a experiencias anteriores?		
12.4.1	Registro de eventos	¿Y a desactivaciones no autorizadas?		
12.4.1	Registro de eventos	¿Y a las interconexiones de los sistemas afectados?		
12.4.1	Registro de eventos	¿Se han establecido procedimientos para la monitorización del uso de los sistemas de información?		
12.4.1	Registro de eventos	¿Se ha decidido lo que hay que monitorizar y con qué nivel apoyándose en el análisis de riesgos?		
12.4.1	Registro de eventos	¿Se monitoriza que los accesos a datos y sistemas sean los autorizados?		
12.4.1	Registro de eventos	¿Y al valor o criticidad de la información procesada?		
12.4.1	Registro de eventos	¿Se mantiene un log de los fallos del sistema de información?		

12.4.1	Registro de eventos	¿Se cuenta con procedimientos para gestionar los fallos reportados?		
12.4.1	Registro de eventos	¿Incluyen indicaciones para asegurar que los fallos se resuelvan?		
12.4.1	Registro de eventos	¿Y la revisión de las acciones correctivas?		
12.4.1	Registro de eventos	¿Se revisa que el log de errores esté activado donde esté disponible?		
12.4.2	Protección de la información de registro	¿Cuenta el sistema con protección frente a cambios en los tipos de mensajes y eventos que se registran?		
12.4.2	Protección de la información de registro	¿Están protegidos tanto los logs como las herramientas que los generan?		
12.4.2	Protección de la información de registro	¿Y a la edición o destrucción de los logs?		
12.4.2	Protección de la información de registro	¿Se tienen en cuenta los requerimientos legales para los registros que pueden ser utilizados como evidencias?		
12.4.2	Protección de la información de registro	¿Y a que se acceda a la capacidad de almacenamiento del sistema donde se almacenan los logs?		
12.4.3	Registros de administración y operación	¿Se revisan periódicamente los logs de los administradores?		
12.4.3	Registros de administración y operación	¿Se mantiene un log de las actividades del administrador del sistema?		
12.4.3	Registros de administración y operación	¿Se registra la fecha y hora del evento?		

12.4.3	Registros de administración y operación	¿Y el tipo de evento?		
12.4.3	Registros de administración y operación	¿Y el tipo de fallo?		
12.4.3	Registros de administración y operación	¿Y el proceso o aplicación involucrada?		
12.4.3	Registros de administración y operación	¿Y el administrador involucrado?		
12.4.4	Sincronización del reloj	¿Se garantiza la trazabilidad horaria de los eventos almacenados en los logs de diferentes sistemas de información?		
12.4.4	Sincronización del reloj	¿Están sincronizados todos los relojes de los ordenadores?		
12.4.4	Sincronización del reloj	¿Se ha acordado una base de tiempos para todos los relojes de tiempo real?		
12.4.4	Sincronización del reloj	¿Se sincronizan periódicamente todos los relojes?		
12.4.4	Sincronización del reloj	¿Se tiene documentada los posibles cambios horarios de todas las delegaciones distribuidas?		
12.5 Control del software en explotación				
12.5.1	Instalación del software en explotación	Si el software es adquirido ¿se tiene en cuenta la seguridad de la versión a la hora de tomar la decisión de paso a nuevas versiones?		
12.5.1	Instalación del software en explotación	¿Se aplica algún control para la implantar software en el sistema en operación?		

12.5.1	Instalación del software en explotación	¿Existen usuarios autorizados para realizar los cambios en los sistemas en producción?		
12.5.1	Instalación del software en explotación	¿Se realizan pruebas de funcionalidad previas en entornos de pruebas?		
12.5.1	Instalación del software en explotación	¿Y pruebas de integración?		
12.5.1	Instalación del software en explotación	¿Existe un proceso de autorización previa a los cambios de SW en producción?		
12.5.1	Instalación del software en explotación	¿Existe un sistema de control de configuración para mantener un control de todo el software puesto en producción así como la documentación del sistema?		
12.5.1	Instalación del software en explotación	¿Existe una estrategia de restauración a la versión anterior?		
12.5.1	Instalación del software en explotación	¿Se mantienen registros de auditoría de los cambios efectuados?		
12.5.1	Instalación del software en explotación	¿Se impide la instalación de código fuente en los sistemas en explotación, limitándolo a la instalación únicamente de ficheros previamente compilados?		
12.5.1	Instalación del software en explotación	¿Son archivadas las versiones obsoletas de software junto con toda la información, parámetros, procedimientos, detalles de configuración, y el software de soporte de los datos mantenidos ?		
12.6 Gestión de la vulnerabilidad técnica				

12.6.1	Gestión de las vulnerabilidades técnicas	Si el parche está disponible ¿se evalúan los riesgos asociados a su instalación?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Existe un procedimiento adecuado para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes, para identificar los riesgos y las acciones a tomar?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se monitoriza y evalúa periódicamente la gestión de vulnerabilidades técnicas?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se evalúa y se prueba el parche antes de su instalación?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se definen y establecen las responsabilidades asociadas con la gestión de vulnerabilidades técnicas?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se incluye, en el inventario de activos, el vendedor del software, número de versión, estado actual del desarrollo (qué software está instalado en qué sistema) y el responsable para el software?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se obtiene información sobre vulnerabilidades técnicas de los sistemas de información y se toman las medidas apropiadas?		

12.6.1	Gestión de las vulnerabilidades técnicas	Si el parche no está disponible ¿Se consideran otros controles, tales como desconexión de servicios o capacidades relacionadas con la vulnerabilidad, adaptando o añadiendo controles de accesos, incrementando la monitorización etc.?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se realizan auditorías periódicas de los procedimientos emprendidos?		
12.6.1	Gestión de las vulnerabilidades técnicas	¿Se mantiene los recursos de la información actualizados en el inventario de activos, para identificar vulnerabilidades técnicas?		
12.6.2	Restricción en la instalación del software	¿Se ha fijado una política de software permitido?		
12.6.2	Restricción en la instalación del software	¿El software que se propone instalar cuenta con el permiso de la organización?		
12.6.2	Restricción en la instalación del software	¿El software que se propone instalar es estrictamente necesario para un desempeño?		
12.7 Consideraciones sobre la auditoria de sistemasde información				
12.7.1	Controles de la auditoria de sistemas de información	¿Se registran los rastros de la auditoría?		
12.7.1	Controles de la auditoria de sistemas de información	¿Están planificadas las auditorías de sistemas para reducir el riesgo de interrupciones en el proceso de negocio?		
12.7.1	Controles de la auditoria de sistemas de información	¿El auditor es independiente de las actividades auditadas?		

	12.7.1	Controles de la auditoria de sistemas de información	¿Se planifica previamente la restauración de los servicios que se vean afectados por la elaboración de la auditoría?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se establecen cláusulas de responsabilidad por desastres producidos por la auditoría?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se revisan posteriormente para comprobar el cumplimiento de lo acordado?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se identifican los sistemas utilizados para realizar la auditoría?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se limita el acceso de la auditoría únicamente a leer la información?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se limita formalmente el alcance de la auditoría?		
	12.7.1	Controles de la auditoria de sistemas de información	¿Se identifican los requisitos para procesos especiales o adicionales?		
13 Seguridad de las comunicaciones	**13.1 Gestión de la seguridad de redes**				
	13.1.1	Controles de red	¿Se han definido las responsabilidades y procedimientos para la gestión remota de equipos?		
	13.1.1	Controles de red	¿Se han implantado controles para mantener la seguridad en la red?		
	13.1.1	Controles de red	¿Están separadas las responsabilidades de red de las de sistemas?		
	13.1.1	Controles de red	¿Se han controles especiales para el uso de redes inalámbricas?		

	13.1.1	Controles de red	¿Se dispone de alguna herramienta de registro y monitorización de lo que ocurre en la red?		
	13.1.2	Seguridad de los servicios de red	¿Están documentadas las características de seguridad, niveles de servicio y requerimientos de gestión de los servicios de red?		
	13.1.2	Seguridad de los servicios de red	¿Se reserva la organización el derecho de auditar al proveedor?		
	13.1.2	Seguridad de los servicios de red	¿Se asegura la organización de que el proveedor implanta los controles de seguridad necesarios?		
	13.1.3	Segregación de redes	¿Se han instalado gateways seguros (normalmente firewalls) entre las redes?		
	13.1.3	Segregación de redes	¿Están segmentadas las redes inalámbricas de las redes interna y externa?		
	13.1.3	Segregación de redes	¿El criterio para la segmentación de la red es coherente con la política de control de accesos?		
	13.1.3	Segregación de redes	¿Se utiliza IP switching?		
	13.1.3	Segregación de redes	¿Se utilizan VPNs para distintos grupos de usuarios?		
	13.1.3	Segregación de redes	¿Se filtra el tráfico entre los distintos segmentos de red?		
	13.1.3	Segregación de redes	¿Se ha tenido en cuenta el análisis de riesgos para definir el nivel de seguridad que se requiere en cada segmento?		
	13.1.3	Segregación de redes	¿Se han definido controles de seguridad proporcionales para cada		

			uno de los segmentos?		
	13.1.3	Segregación de redes	¿Y en las que se sitúan los servicios críticos internos?		
	13.1.3	Segregación de redes	¿Se encuentran separadas las redes con servicios internos de las que soportan servicios externos?		
	13.1.3	Segregación de redes	¿Está la red segmentada por grupos usuarios y servicios?		
	13.1.3	Segregación de redes	¿Se bloquean los intentos de acceso no autorizado?		
	13.2 Intercambio de información				
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se utilizan técnicas criptográficas en el intercambio de información sensible?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se han proporcionado guías a los empleados y terceras partes para el almacenamiento y destrucción de correspondencia?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se han dado indicaciones expresas para que los usuarios no dejen copias de información sensible en impresoras, fotocopiadoras, faxes, etc.?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se han implantado controles para los reenvíos automáticos de información, por ejemplo email o desvió de llamadas?		

	13.2.1	Políticas y procedimientos de intercambio de información	¿Se han dado indicaciones expresas para que los usuarios no comenten información sensible en sus llamadas telefónicas sin verificar quien puede estar escuchando?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Y con respecto al envío de faxes por ejemplo a un número equivocado o a una persona que no está disponible para recibirlo?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se establecen cláusulas de responsabilidad para los empleados y terceras partes en el intercambio de información o software (difamaciones, vulneraciones de los derechos de propiedad intelectual, compras no autorizadas, etc.)?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Y para que no den información sensible en mensajes dejados en contestadores automáticos, tablones de anuncios, etc.?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Y con respecto a la memoria interna y cache de algunas impresoras, fotocopiadoras y faxes?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Se protege la información sensible adjuntada a un correo electrónico?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Y frente a destrucción?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Y frente a errores de enrutamiento o envío?		

	13.2.1	Políticas y procedimientos de intercambio de información	¿Y frente a copia?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Existen procedimientos formales para regular el intercambio de información?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Existen procedimientos para el uso de redes inalámbricas para intercambio de información sensible con terceros?		
	13.2.1	Políticas y procedimientos de intercambio de información	¿Existen procedimientos para proteger la información intercambiada frente a intercepciones?		
	13.2.2	Acuerdos de intercambio de información	¿Y los aspectos técnicos para leer la información o ejecutar el software?		
	13.2.2	Acuerdos de intercambio de información	¿Y los aspectos relacionados con la propiedad intelectual, licencias, copyright, etc.?		
	13.2.2	Acuerdos de intercambio de información	¿Y el uso de un etiquetado especifico?		
	13.2.2	Acuerdos de intercambio de información	¿Y las responsabilidades en caso de pérdidas de información?		
	13.2.2	Acuerdos de intercambio de información	¿Y los aspectos técnicos para el empaquetado y la transmisión?		
	13.2.2	Acuerdos de intercambio de información	¿Y para asegurar la trazabilidad y el no repudio?		
	13.2.2	Acuerdos de intercambio de información	¿Contempla estos acuerdos la propiedad de la información intercambiada?		
	13.2.2	Acuerdos de intercambio de información	¿Y las responsabilidades a la finalización del acuerdo?		

	13.2.2	Acuerdos de intercambio de información	¿Se han tenido en cuenta en los acuerdos las responsabilidades para controlar y notificar las transmisiones y recepciones de información sensible en tránsito?		
	13.2.2	Acuerdos de intercambio de información	¿Se han establecido acuerdos con otras empresas para intercambiar información o aplicaciones?		
	13.2.3	Mensajería electrónica	¿Se pide algún tipo de autenticación especial cuando se accede a mensajería electrónica a través de redes públicas?		
	13.2.3	Mensajería electrónica	¿Existe una política para el uso de la mensajería electrónica (email, EDI, messenger, etc.)?		
	13.2.3	Mensajería electrónica	¿Están protegidos los mensajes contra accesos no autorizados?		
	13.2.3	Mensajería electrónica	¿Y frente a modificaciones?		
	13.2.3	Mensajería electrónica	¿Y frente a denegación de servicio?		
	13.2.3	Mensajería electrónica	¿Se asegura la dirección de destino de los mensajes?		
	13.2.3	Mensajería electrónica	¿Se han previsto los requisitos legales para el uso de firma electrónica en mensajes electrónicos?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Y para todos los usuarios que en general no disponen de un contrato laboral?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifican y revisan regularmente los requerimientos de los acuerdos de confidencialidad o no		

			divulgación de la organización?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Firman los empleados un acuerdo de confidencialidad?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifican las condiciones de devolución o destrucción de la información a la finalización del acuerdo o la relación laboral con el empleado?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Y para usuarios de terceros?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se incluyen los procesos para notificación de las divulgaciones no autorizadas de la información confidencial?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Contienen los acuerdos de confidencialidad la definición de la información que debe ser protegida?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifica la duración del acuerdo de confidencialidad?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifican las acciones requeridas cuando finalizan los acuerdos de confidencialidad?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifican las responsabilidades y acciones de los firmantes para evitar divulgación no autorizada de la información?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se identifica el uso permitido de la información confidencial y los derechos de los firmantes para el uso de		

			la información?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se incluye el derecho de auditar y las actividades de monitorización que involucran la información confidencial?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se revisan las cláusulas de confidencialidad periódicamente o cuando existan cambios en los requerimientos?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Permite el contrato la modificación o ampliación de los requerimientos y procedimientos de seguridad?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Los acuerdos de confidencialidad cumplen con todas las leyes y regulaciones aplicables por la jurisdicción?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se incluyen otros requerimientos de seguridad necesarios por la organización en los acuerdos de confidencialidad?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿y las acciones a tomar en caso de no cumplimiento del acuerdo?		
	13.2.4	Acuerdos de confidencialidad o no revelación	¿Se requiere la firma de un acuerdo de confidencialidad para personal subcontratado?		
desarrollo y mantenimiento de los sistemas	**14.1 Requisitos de seguridad en sistemas de la información**				
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	¿Se especifican los controles de seguridad necesarios para nuevos sistemas o mejoras de los actuales?		

	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Si la funcionalidad de la seguridad en un producto propuesto no satisface el requisito especificado ¿los controles introducidos y asociados del riesgo se deben reconsiderar antes de comprar el producto?		
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Si el producto es comprado ¿se identifican los requerimientos de seguridad en los contratos?		
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	¿Se requiere la aprobación del comité para adquirir nuevos sistemas?		
	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	¿Y en la adquisición o desarrollo de nuevo software que interviene en los procesos de los sistemas de información?		
	14.1.2	Comercio electrónico	¿Se garantiza la confidencialidad e integridad de todas las transacciones asociadas a la operación (pedidos, pagos, facturas, dirección de envío, confirmación de recepción, etc.)?		
	14.1.2	Comercio electrónico	¿Y el nivel de confidencialidad de la información sensible asociada a las operaciones de comercio electrónico?		
	14.1.2	Comercio electrónico	¿Se ha establecido el nivel de confianza necesario en la integridad de las listas de precios?		
	14.1.2	Comercio electrónico	¿Se asegura que ambas partes están informadas de sus autorizaciones?		

	14.1.2	Comercio electrónico	¿Se han establecido procesos sobre quién puede establecer precios, publicar documentos o firmar acuerdos?		
	14.1.2	Comercio electrónico	¿Se ha establecido el nivel de autenticación requerido para cada una de las partes?		
	14.1.2	Comercio electrónico	¿Está protegida la información relacionada con comercio electrónico que utiliza redes públicas contra actividades fraudulentas, disputas contractuales y difusiones no autorizadas?		
	14.1.2	Comercio electrónico	¿Y de la entrega de la adquisición?		
	14.1.2	Comercio electrónico	¿Se verifican las condiciones de los contratos?		
	14.1.2	Información públicamente disponible	¿Existe un proceso formal de aprobación antes de que la información se publique?		
	14.1.2	Información públicamente disponible	¿Se prueban los sistemas que alojan información pública para verificar que no tienen debilidades o fallos?		
	14.1.2	Información públicamente disponible	¿Se verifican y aprueban las aportaciones externas antes de publicarlas?		
	14.1.2	Información públicamente disponible	¿Se controlan los sistemas que publican la información para verificar que la información publicada cumple con los requerimientos legales?		
	14.1.2	Información públicamente disponible	¿Y que los procesos relacionados con la publicación de la información se completan?		

	14.1.2	Información públicamente disponible	¿Y que la información sensible está protegida durante los procesos de recogida, procesado y almacenamiento?		
	14.1.2	Información públicamente disponible	¿Se dispone de controles que garanticen que desde los sistemas públicos no se puede acceder a otros entornos de red a los que estos sistemas estén conectados?		
	14.1.2	Información públicamente disponible	¿Se protege la integridad de la información publicada para prevenir modificaciones no autorizadas?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se utilizan autoridades de confianza?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se tienen en cuenta los requerimientos legales de los países donde se encuentran ambas partes?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Son seguros los protocolos utilizados en la comunicación?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Están cifradas las comunicaciones entre todas las partes involucradas en la transacción?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se garantía la privacidad de ambas partes?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se garantiza la confidencialidad de la transacción?		
	14.1.3	Protección de las transacciones de servicios de	¿Se verifica que las credenciales de ambas partes son válidas?		

		aplicaciones			
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se almacenan los datos de la transacción en un entorno no accesible públicamente?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Se requiere el uso de las firmas electrónicas de ambas partes?		
	14.1.3	Protección de las transacciones de servicios de aplicaciones	¿Esta protegida la información de las transacciones en línea?		
	14.2 Seguridad en el desarrollo y en los procesos de soporte				
	14.2.1	Política de desarrollo seguro	¿Se informa y registra cualquier desarrollo de aplicaciones y sistemas internos?		
	14.2.1	Política de desarrollo seguro	¿Las aplicaciones y sistemas internos cumplen todas las reglas de seguridad?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se mantiene un registro de las necesidades de los usuarios en cuanto a actualizaciones de versiones?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se complementan los cambios con la información y formación necesaria?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se asegura la actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua?		

	14.2.2	Procedimientos de control de cambios en sistemas	¿Se asegura que el proceso de cambios se realiza de forma que minimice el impacto en el funcionamiento de la organización?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se recopilan las aprobaciones de los cambios de los usuarios antes y después de efectuarlos?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se mantiene un control de versiones de toda la actualización del software?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se asegura que los cambios únicamente se realizan por usuarios debidamente autorizados?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se mantienen registros de las solicitudes y cambios efectuados?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se mantiene un registro de los niveles de autorización acordados para la ejecución de los cambios?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se asegura que en el proceso de cambios se realiza un análisis de riesgo y de los impactos de cambios, y los requerimientos de los controles de la seguridad necesarios?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Existen procedimientos para el control de cambios?		
	14.2.2	Procedimientos de control de cambios en sistemas	¿Se mantienen registros de SW y HW para controlar que usuarios son los afectados en un proceso de cambio?		

	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se asegura que se realizan los cambios apropiados en los planes de continuidad del negocio?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Existen responsables para realizar los cambios en el SO?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se asegura que el proceso de cambios se realiza de forma que minimice el impacto en el funcionamiento de la organización?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se realizan jornadas de formación en los casos en los que son necesarios?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se elaboran y distribuyen procedimientos o manuales asociados a los cambios en el SO?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se contemplan las necesidades de soporte externo cuando se realiza un cambio de SO?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se realizan pruebas de funcionalidad e integración con el resto de sistemas?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se impide que los usuarios realicen cambios en el SO, tales como instalación de parches de actualización o cambios de versiones?		
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se revisan y aprueban los sistemas de aplicación cuando se producen cambios en el sistema operativo?		

	14.2.4	Restricciones a los cambios en los paquetes de software	¿Se intenta previamente obtener los cambios necesarios directamente del proveedor o fabricante?		
	14.2.4	Restricciones de los cambios a los paquetes de software	¿Se registran, prueban y documentan las modificaciones efectuadas?		
	14.2.4	Restricciones de los cambios a los paquetes de software	¿Se desaconsejan o limitan a los cambios necesarios las modificaciones de los paquetes de software?		
	14.2.4	Restricciones de los cambios a los paquetes de software	¿Se almacena el SW original?		
	14.2.5	Principios de ingeniería de sistemas seguros	¿Se han fijado unos criterios para considerar un sistema de ingeniería seguro?		
	14.2.5	Principios de ingeniería de sistemas seguros	¿Se han documentado estos principios?		
	14.2.5	Principios de ingeniería de sistemas seguros	¿Se garantiza su mantenimiento a lo largo del tiempo?		
	14.2.6	Entorno de desarrollo seguro	¿Está garantizada la seguridad del lugar físico donde se lleva a cabo el desarrollo?		
	14.2.6	Entorno de desarrollo seguro	¿El sistema estará protegido a lo largo de todo su ciclo de vida?		
	14.2.7	Externalización del desarrollo de software	¿Y de derechos de acceso a los fuentes para someterlos a auditorias?		
	14.2.7	Externalización del desarrollo de software	¿Y de acceso a los fuentes en caso de disputas, conflictos o continuidad?		
	14.2.7	Externalización del desarrollo de software	¿Se regulan acuerdos de licencias y derechos de propiedad del código desarrollado?		

	14.2.7	Externalización del desarrollo de software	¿Se aplican controles para asegurar que el desarrollo subcontratado de software cumple con las medidas de seguridad necesarias?		
	14.2.7	Externalización del desarrollo de software	¿Se realizan pruebas antes de la implantación para detectar código malicioso y Troyano?		
	14.2.7	Externalización del desarrollo de software	¿Se exigen acuerdos de responsabilidad, de garantía o calidad sobre los trabajos contratados?		
	14.2.8	Pruebas funcionales de seguridad de sistemas	¿Se han efectuado pruebas a la seguridad durante el desarrollo?		
	14.2.8	Pruebas funcionales de seguridad de sistemas	¿Dichas pruebas concuerdan con los criterios esperados de las mismas?		
	14.2.8	Pruebas funcionales de seguridad de sistemas	¿Esas pruebas han sido superadas satisfactoriamente?		
	14.2.9	Pruebas de aceptación de sistemas	¿Y los aspectos relacionados con la continuidad de negocio?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se cuenta con algún proceso formal de acreditación o certificación que verifique que el nuevo sistema cumple con todos los requerimientos de seguridad?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se ha tenido en cuenta la facilidad de uso del nuevo sistema?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se solicitan evidencias de que la instalación del nuevo sistema no afectara negativamente a los sistemas existentes?		
	14.2.9	Pruebas de aceptación de	¿Y la existencia de un grupo concreto de		

		sistemas	controles de seguridad asociados?		
	14.2.9	Pruebas de aceptación de sistemas	¿Y los planes de contingencia?		
	14.2.9	Pruebas de aceptación de sistemas	¿Y los procedimientos de recuperación de errores?		
	14.2.9	Pruebas de aceptación de sistemas	¿Existen criterios de aceptación para nuevos sistemas, ampliaciones o nuevas versiones?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se tiene en cuenta el rendimiento y los requisitos de capacidad de los ordenadores antes de aceptar formalmente el nuevo sistema?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se garantiza que no se pasan los nuevos sistemas a producción hasta obtener la aprobación formal?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se asegura la dirección de que los requerimientos y criterios para la aceptación de nuevos sistemas son los adecuados?		
	14.2.9	Pruebas de aceptación de sistemas	¿Y los procedimientos de reinicio?		
	14.2.9	Pruebas de aceptación de sistemas	¿Se tiene en cuenta si se ha impartido la formación necesaria para operar el nuevo sistema?		
	14.3 Datos de prueba				
	14.3.1	Protección de los datos de prueba	¿Están protegidos los datos de prueba?		
	14.3.1	Protección de los datos de prueba	¿Se autoriza formalmente el uso de información en sistemas de prueba?		

	14.3.1	Protección de los datos de prueba	¿Se establecen previamente los controles de acceso necesarios a la información y sistemas de información de los entornos de prueba?		
	14.3.1	Protección de los datos de prueba	En los casos que sea posible, ¿se utilizan datos ficticios para realizar las pruebas?		
	14.3.1	Protección de los datos de prueba	¿Se registra el uso de los datos de prueba?		
	14.3.1	Protección de los datos de prueba	¿Se realizan revisiones periódicas de los registros de acceso a los sistemas de información en prueba?		
	14.3.1	Protección de los datos de prueba	¿Se elimina la información de forma segura una vez finalizados todos los procesos de prueba?		
	14.3.1	Protección de los datos de prueba	¿Se registra la copia y eliminación de los datos de prueba?		
15 Relación con proveedores	**15.1 Seguridad en las relaciones con proveedores**				
	15.1.1	Política de Seguridad de la información en las relaciones con los proveedores	¿Se han definido unos requisitos asociados al acceso de activos de la empresa?		
	15.1.1	Política de Seguridad de la información en las relaciones con los proveedores	¿Se han acordado con proveedor dichos requisitos para el acceso a los activos de la organización?		
	15.1.1	Política de Seguridad de la información en las relaciones con los proveedores	¿Quedan documentados estos requisitos y reconocidos por organización y proveedor?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿El derecho de auditar?		

	15.1.2	Requisitos de seguridad en contratos con terceros	¿Se ha valorado e incluido en el contrato con terceros los aspectos relacionados con la seguridad de la información?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Cómo cumplimentar los requerimientos legales?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Cómo asegurar que las partes implicadas en la externalización, incluidos los subcontratistas, conocen sus responsabilidades en materia de seguridad?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Los controles que se implantarán para mantener la integridad y confidencialidad?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Los controles físicos y lógicos se van a utilizar para controlar el acceso a la información sensible?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Los niveles de seguridad física que deben proporcionarse al equipamiento externalizado?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Permite el contrato la modificación o ampliación de los requerimientos y procedimientos de seguridad?		
	15.1.2	Requisitos de seguridad en contratos con terceros	¿Los procedimientos para mantener la disponibilidad de los servicios en caso de desastre?		
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	¿Se han definido unos requisitos de seguridad de tecnologías de la información para hacer frente a los posibles riesgos?		

	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	¿Se han definido unos requisitos de seguridad en las comunicaciones para hacer frente a los posibles riesgos?		
	15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	¿Se han definido unos requisitos de seguridad con la cadena de suministro para frente a los posibles riesgos?		
	15.2 Gestión de la provisión de servicios del proveedor				
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se revisan y auditan periódicamente los informes y registros suministrados por el proveedor del servicio?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se ha asignado la responsabilidad de la gestión de las relaciones con la tercera parte a una persona o a un equipo de personas?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se revisan las evidencias y registros de auditoria de seguridad de la tercera parte con respecto a la seguridad de los servicios suministrados?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se mantienen regularmente reuniones de seguimiento?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se revisan los informes de servicio elaborados por la tercera parte?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se cuenta con los perfiles técnicos adecuados para comprobar si se están cumpliendo con los compromisos en materia de seguridad?		

	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se monitoriza que los términos y condiciones en materia de seguridad de la información del acuerdo se estén cubriendo?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se adoptan acciones correctivas cuando se detectan deficiencias?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se monitoriza que se haga una gestión adecuada de los incidentes y problemas de seguridad?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Mantiene la organización visibilidad de las actividades de seguridad desarrolladas por la tercera parte?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se mantiene visibilidad de la gestión de cambios?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Y de la identificación de vulnerabilidades?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Y de la gestión de incidentes?		
	15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se ha verificado si la tercera parte Ha asignado a su vez la responsabilidad de la gestión de las relaciones a una persona o a un equipo de personas?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el desarrollo de nuevos servicios?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el cambio de la ubicación física de las instalaciones desde las que se presta el servicio?		

	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el desarrollo de nuevas herramientas o entornos?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el uso de nuevos productos o actualización de versiones?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el uso de nuevas tecnologías?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Se tienen en cuenta los cambios realizados por la tercera parte para implantar cambios y mejoras en las redes?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y las modificaciones o actualizaciones de las políticas y procedimientos de la organización?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y el cambio de proveedores?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Se tiene en cuenta los cambios desarrollados por la organización para mejorar los servicios suministrados?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Se dispone de un procedimiento para la gestión de cambios de los servicios suministrados por la tercera parte?		
	15.2.2	Gestión de cambios en la provisión del servicio del proveedor	¿Y nuevos controles para solventar los incidentes de seguridad?		
de incidentes de seguridad de la	**16.1 Gestión de incidentes de seguridad de la información y mejoras**				
	16.1.1	Responsabilidades y procedimientos	¿Se confirma el correcto funcionamiento del sistema tras una intervención?		

	16.1.1	Responsabilidades y procedimientos	¿Se comunica a los afectados la recuperación de la incidencia?		
	16.1.1	Responsabilidades y procedimientos	¿Y de código malicioso?		
	16.1.1	Responsabilidades y procedimientos	¿Se registran las acciones efectuadas en la gestión de un incidente?		
	16.1.1	Responsabilidades y procedimientos	¿Se han establecido procedimientos y responsabilidades, para la gestión de incidentes?		
	16.1.1	Responsabilidades y procedimientos	¿Existe un canal aprobado de notificación de incidentes de seguridad?		
	16.1.1	Responsabilidades y procedimientos	¿Se recogen los fallos detectados en los sistemas?		
	16.1.1	Responsabilidades y procedimientos	¿Se aplican normas disciplinarias cuando procede?		
	16.1.1	Responsabilidades y procedimientos	¿Y en la degradación de servicios?		
	16.1.1	Responsabilidades y procedimientos	¿Y de errores de datos recogidos?		
	16.1.1	Responsabilidades y procedimientos	¿Y de violaciones de confidencialidad y de integridad?		
	16.1.1	Responsabilidades y procedimientos	¿Y de mal uso de sistemas de información?		
	16.1.1	Responsabilidades y procedimientos	¿Existen procedimientos para recuperar rápidamente el sistema a su estado anterior?		
	16.1.1	Responsabilidades y procedimientos	¿Se analiza e identifica la causa de la incidencia?		
	16.1.1	Responsabilidades y procedimientos	¿Se analizan los fallos reportados para evitar su repetición?		
	16.1.1	Responsabilidades y procedimientos	¿Y a la dirección, al responsable directo o al propietario de los activos afectados?		

	16.1.1	Responsabilidades y procedimientos	¿Existen cláusulas de responsabilidad para terceros por fallos en los sistemas?		
	16.1.1	Responsabilidades y procedimientos	¿Y en las aplicaciones?		
	16.1.2	Notificación de los eventos de seguridad de la información	En entornos de alto riesgo ¿existen alarmas bajo coacción y procedimientos para responder ante coacción?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Existe un proceso disciplinario para tratar las violaciones de las políticas y procedimientos de seguridad?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Existe un canal a través del que se reporten los incidentes de seguridad?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Existe un procedimiento para informar de las incidencias de seguridad?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Y de respuesta a incidencias?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Conocen todos los empleados, contratados y terceras partes el procedimiento para informar de las incidencias?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Existe un procedimiento de acuse de recibo para estas notificaciones de incidencias?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Y para notificar de la resolución de la misma?		
	16.1.2	Notificación de los eventos de seguridad de la	¿Y para los casos del equipamiento y usuarios externalizados?		

		información			
	16.1.2	Notificación de los eventos de seguridad de la información	¿Se les indica a los usuarios que no traten de realizar una acción propia para intentar resolver la incidencia de seguridad?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Se notifica periódicamente las consecuencias de infringir las normas de seguridad como recordatorio?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Conocen los usuarios la existencia de alarmas bajo coacción?		
	16.1.2	Notificación de los eventos de seguridad de la información	¿Se notifican todos los detalles importantes (ej; tipo de incumplimiento, mensajes en pantalla, comportamientos extraños etc...) de la incidencia de seguridad inmediatamente, para ayudar a resolverla?		
	16.1.3	Notificación de puntos débiles de la seguridad	¿Se solicita a los empleados, contratistas y terceros que comuniquen cualquier debilidad de seguridad o amenaza para el sistema?		
	16.1.3	Notificación de puntos débiles de la seguridad	¿Se les indica a los usuarios que no traten de verificar si la amenaza es real?		
	16.1.3	Notificación de puntos débiles de la seguridad	¿Existe un procedimiento para informar de las debilidades de seguridad?		
	16.1.3	Notificación de puntos débiles de la seguridad	¿Conocen todos los empleados, contratados y terceras partes el procedimiento para informar de las debilidades?		

	16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	¿Los sucesos que comprometen la seguridad son evaluados?		
	16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	¿Tras estas evaluaciones se opta por que sean clasificados como incidentes de la seguridad de la información?		
	16.1.5	Respuesta a incidentes de seguridad de la información	¿Están claros los procedimientos documentados relacionados con la gestión de incidentes?		
	16.1.5	Respuesta a incidentes de seguridad de la información	¿Las incidencias se gestionan acorde con estos procedimientos?		
	16.1.6	Aprendizaje de los incidentes de la seguridad de la información	¿Se analizan los tipos, volúmenes y costes de los incidentes y fallos?		
	16.1.6	Aprendizaje de los incidentes de la seguridad de la información	¿Se hacen informes periódicos de las incidencias más habituales o con mayor impacto?		
	16.1.6	Aprendizaje de los incidentes de la seguridad de la información	¿Analiza el comité de seguridad estos informes?		
	16.1.7	Recopilación de evidencias	Para apoyar una acción contra una persona u organización ¿Se mantienen las evidencias, conforme a las leyes y normas publicadas?		
	16.1.7	Recopilación de evidencias	¿Se almacenan de forma que no se pueda comprometer la confidencialidad, integridad y disponibilidad?		

	16.1.7	Recopilación de evidencias	¿Se recogen pruebas y evidencias que puedan servir ante las autoridades o tribunales?		
	16.1.7	Recopilación de evidencias	¿Se disponen de herramientas forenses para analizar los usos de los sistemas de información?		
	16.1.7	Recopilación de evidencias	Cuando la acción sea materia disciplinaria interna ¿Se describe en procedimientos internos?		
17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	**17.1 Continuidad de la seguridad de la información**				
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Existe un responsable encargado de mantener y revisar los Análisis de Riesgos?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se ha contemplado en el análisis de riesgos las premisas Confidencialidad, Integridad y Disponibilidad?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se han inventariado y valorado todos los activos críticos de negocio?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se ha considerado también los bienes intangibles?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se han valorado las amenazas y las vulnerabilidades a las que están expuestos estos activos?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se encuentran categorizados los riesgos detectados en el análisis?		
	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Se han implantado los controles adecuados para minimizar los riesgos a niveles asumibles por la organización?		

	17.1.1	Planificación de la continuidad de la seguridad de la información	¿Existe un plan estratégico, basado en la valoración de riesgos, donde se detallen las acciones para la continuidad del negocio?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se considera la seguridad de empleados y la protección de instalaciones de tratamiento de información en el PCN?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se encuentra el PCN accesible en todo momento a todos los responsables de llevar a cabo sus tareas de responsabilidad, incluso ante una situación de desastre?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Contempla el PCN los recursos financieros, organizacionales, técnicos y ambientales suficientes?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se considera la implantación de controles adicionales preventivos o correctivos en el PCN?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se considera la adquisición de los seguros adecuados que forman parte del PCN?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Contempla el PCN todos los activos implicados en los procesos críticos de la organización?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Contempla el PCN todos los procesos críticos de la organización que puedan poner en peligro la continuidad ante un desastre?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Existe un proceso establecido en la organización, para desarrollar y mantener la		

			continuidad del negocio?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Están desarrollados los planes de continuidad para mantener o restaurar las operaciones del negocio en un tiempo razonable?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se identifica la pérdida aceptable de información y servicios?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se identifican los procedimientos a seguir hasta la recuperación y restauración de la actividad normal?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se realiza la formación apropiada a todos los responsables de llevar a cabo sus tareas de responsabilidad, en los procedimientos y procesos de emergencia acordados?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se ha establecido un canal para tramitar las solicitudes de modificación o mejora de los PCN?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se encuentra el PCN almacenado en un sitio protegido y seguro?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se dispone de una copia del PCN almacenada a suficiente distancia para no verse afectado por cualquier desastre en el sitio original?		

	17.1.2	Implementar la continuidad de la seguridad de la información	¿El lugar alternativo de almacenamiento de la copia del PCN está protegido con el mismo nivel de seguridad que es aplicado al lugar principal?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Existe un responsable encargado de mantener y revisar los PCN?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Existe un plan general de trabajo para asegurar que todos los planes son consistentes?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se realizan rotaciones en la asignación de tareas implicadas en los PCN con el fin de que al menos 2 personas conozcan las tareas encomendadas?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Se especifican claramente las condiciones para la activación del PCN, así como los responsables de ejecutar cada etapa del plan?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Están priorizadas las fases de restauración ante una contingencia?		
	17.1.2	Implementar la continuidad de la seguridad de la información	¿Conocen todos los implicados las tareas encomendadas?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se revisan los resultados posteriormente con el fin de mejorar los PCN?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se prueban regularmente los planes de continuidad de negocio para asegurar que son eficaces?		

	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se asignan responsabilidades para revisar regularmente cada PCN?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se realizan revisiones y actualizaciones regulares del PCN para asegurar la continuidad de su eficacia?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Son conscientes los empleados del grado de colaboración necesario para actuar ante una situación de contingencias?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se elabora un calendario de pruebas para indicar cómo y cuándo probar cada elemento del plan?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Colaboran todos los empleados en las pruebas del PCN?		
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se documentan los resultados obtenidos de las pruebas efectuadas con las personas que intervienen, responsables, tiempos, etc.?		
	17.2 Redundancias				
	17.2.1	Disponibilidad de los recursos de tratamiento de la información	¿Está disponible cualquier información que pueda ser solicitada?		
	17.2.1	Disponibilidad de los recursos de tratamiento de la información	¿Queda claro que es preferible una redundancia de información que una falta de la misma?		
	17.2.1	Disponibilidad de los recursos de tratamiento de la información	¿Se mantiene una duplicidad de la información cuya seguridad sea		

			independiente?		
18 Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales				
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Se realizan revisiones y actualizaciones periódicas de esta información?		
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Existe un departamento legal o en su defecto asesores externos que ayude a la organización en materias legales?		
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Existe un responsable para mantener esta documentación?		
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Se han contemplado todos los requisitos, tanto nacionales para relaciones locales, como internacionales para relaciones exteriores?		
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Están definidos y documentados, para cada sistema de información, todos los requisitos legales, regulatorios y contractuales?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Existen controles que aseguren que no se instala material no autorizado en los equipos?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se contemplan las especificaciones de uso del material descargado de Internet?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Existe una política de mantenimiento de las condiciones adecuadas bajo licencia?		

	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se realizan los trámites adecuados para el registro de los desarrollos internos y la elaboración de las cláusulas que protegen los DPI?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se identifican todos los activos con requerimientos de DPI?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se etiquetan adecuadamente los soportes que contienen material con DPI?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se realizan jornadas de concienciación sobre la política de DPI y la intención de adoptar medidas disciplinarias para el personal que lo incumpla?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se mantienen de forma segura los contratos o documentos que acreditan los derechos sobre el material adquirido?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Se adquiere el software de fuentes totalmente confiables?		
	18.1.2	Derechos de propiedad intelectual (DPI)	¿Hay procedimientos para asegurar el cumplimiento con las restricciones legales en el uso de material referente a los derechos de propiedad intelectual y en el uso de productos registrados de software?		
	18.1.3	Protección de los registros de la organización	¿Y de los sistemas de cifrado, claves públicas y privadas?		
	18.1.3	Protección de los registros de la organización	¿Están protegidos contra pérdida, destrucción y falsificación los registros importantes?		

	18.1.3	Protección de los registros de la organización	¿Se destruyen los registros que lo necesitan a su vencimiento?		
	18.1.3	Protección de los registros de la organización	¿Se ha clasificado adecuadamente esta información y se le han aplicado los controles (protección de registros contra pérdida, destrucción o falsificación) correspondientes a su categoría?		
	18.1.3	Protección de los registros de la organización	¿Existen procedimientos sobre retención, almacenamiento, tratamiento y eliminación de los registros y la información?		
	18.1.3	Protección de los registros de la organización	Cuando se utilicen medios electrónicos de almacenamiento, ¿existen procedimientos que aseguren la capacidad de acceso a los datos durante el plazo de retención?		
	18.1.3	Protección de los registros de la organización	¿Se ha contemplado la posibilidad de desastre o degradación que afecte a estos registros y se ha establecido un procedimiento de restauración de los mismos?		
	18.1.3	Protección de los registros de la organización	¿Se tienen presentes los requerimientos legales a la hora de mantener registros de la organización, p.e. los registros financieros, de ex empleados, de auditoría, etc.?		

	18.1.3	Protección de los registros de la organización	¿Existe un calendario formal a disposición de las personas implicadas que identifique las retenciones a las que está sujeta cada tipo de registro?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Se mantienen los registros de incidencias?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Se obtienen los permisos adecuados para realizar transferencia internacional de datos cuando sean necesarios?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Se atienden las solicitudes de los afectados en forma y plazo según se establece en la LOPD?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Se realizan las auditorías establecidas en la LOPD?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Se han obtenido y se almacenan adecuadamente las autorizaciones de los afectados para el tratamiento de los datos personales?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Están identificados y notificados al RGPD todos los ficheros con datos personales?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Existe el preceptivo documento de seguridad?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Existen controles eficaces, para proteger la información personal en base a la legislación vigente?		

	18.1.4	Protección y privacidad de la información de carácter personal	¿Se ha desarrollado la adecuación a la LOPD y RMS?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Conocen todos los empleados relacionados con el tratamiento de datos personales sus obligaciones?		
	18.1.4	Protección y privacidad de la información de carácter personal	¿Existen los procedimientos que permiten el cumplimiento y están disponibles para los empleados?		
	18.1.5	Regulación de los controles criptográficos	¿Se contemplan las restricciones en el uso de controles criptográficos?		
	18.1.5	Regulación de los controles criptográficos	¿Existen controles para asegurar el cumplimiento con los acuerdos, leyes y reglamentos nacionales para controlar el uso de cifrado?		
	18.1.5	Regulación de los controles criptográficos	¿Y de HD con controles criptográficos?		
	18.1.5	Regulación de los controles criptográficos	¿Se dispone de asesoramiento legal para asegurar el cumplimiento de la legislación del país, así como antes de trasladar a otro país información cifrada o controles de cifrado?		
	18.1.5	Regulación de los controles criptográficos	¿Se contemplan las especificaciones para la importación o exportación de SW?		
	18.2 Revisiones de la seguridad de la información				
	18.2.1	Revisión independiente de la seguridad de la información	¿Realiza revisiones algún consultor u organización independiente?		

	18.2.1	Revisión independiente de la seguridad de la información	¿Se realizan revisiones independientes de la implantación de la seguridad?		
	18.2.1	Revisión independiente de la seguridad de la información	¿Realiza revisiones el departamento interno de auditoría?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	Si se detectan incumplimientos o no conformidades ¿Se determinan las causas por parte de la Dirección?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Asegura la dirección que se siguen correctamente los procedimientos de seguridad, dentro de su área de responsabilidad?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se realizan revisiones regulares por parte de la Dirección que aseguren el cumplimiento de las políticas, normas y otros requerimientos de seguridad?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se guardan registros de las revisiones?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Y se evalúan las acciones para asegurar la no repetición de dichos incumplimientos?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se determinan e implementan las acciones correctivas apropiadas?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se revisan las acciones correctivas tomadas?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se guardan y mantienen los registros de las acciones correctivas?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se distribuyen los resultados de las revisiones y las acciones a aquellas personas que sean responsables o se		

			vean afectadas?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se analizan y se realizan mejoras del sistema?		
	18.2.2	Cumplimiento de las políticas y normas de seguridad	¿Se realizan auditorías internas de la gestión de la seguridad?		
	18.2.3	Comprobación del cumplimiento técnico	¿Existe un registro del resultado de revisiones técnicas?		
	18.2.3	Comprobación del cumplimiento técnico	¿Se chequean regularmente los sistemas de información para verificar el cumplimiento con los estándares de implantación de seguridad?		
	18.2.3	Comprobación del cumplimiento técnico	¿Se dispone de herramientas de auditoría técnica de sistemas?		
	18.2.3	Comprobación del cumplimiento técnico	¿Existe un calendario formal para realizar las revisiones técnicas?		
	18.2.3	Comprobación del cumplimiento técnico	¿Se realizan pruebas adicionales periódicas de seguridad, p.e. test de intrusiones externos o análisis de vulnerabilidades?		

Sub-Cláusula 6.2. Objetivos de seguridad de la información y planificación para su consecución

Objetivos de seguridad de la información y planificación para su consecución

DOCUMENTACIÓN PROPUESTA

OBJETO

Este procedimiento define la metodología empleada por LA ORGANIZACIÓN para establecer y documentar los objetivos y metas del Sistema Integrado de Gestión (en adelante SGSI), así como para establecer y mantener al día los programas y planes de gestión establecidos para su consecución.

ALCANCE

Este procedimiento es de aplicación a las actividades desarrolladas por LA ORGANIZACIÓN para definir, establecer y evaluar el cumplimiento de los objetivos y metas del SIG.

DOCUMENTACIÓN DE REFERENCIA

- Norma *ISO/IEC 27001:2013*

ÍNDICE

1. Generalidades

En el contexto de la documentación del SGSI y, en particular, de este procedimiento, se utilizan las siguientes definiciones:

Objetivo: fin de carácter general que tiene su origen en la política de gestión del LA ORGANIZACIÓN. Es coherente con ésta, medible y, siempre que sea posible, cuantificable. Tendrá en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y tratamiento de riesgos. Podrán ser comunicados y actualizados.

Meta: requisito de desempeño detallado aplicable al LA ORGANIZACIÓN, que tiene su origen en los objetivos y que debe establecerse y cumplirse para poder alcanzarlos.

Programa de gestión: planificación documentada de acciones a realizar para alcanzar los objetivos y metas establecidos. En el programa de gestión se incluye la asignación de responsabilidades y los medios y plazos necesarios.

Plan de gestión: establece la planificación relativa procesos necesarios para la gestión del servicio prestado por la organización, así como los objetivos propuestos y los recursos y plazos estimados para su consecución.

2. Procedimiento

2.1 Establecimiento y cumplimiento de objetivos

El Comité de Gestión define, en la reunión de revisión por dirección, los objetivos y metas para ese año, reflejándolos en el acta de reunión correspondiente.

En el establecimiento de los objetivos se considera, al menos, lo siguiente:

- Compromisos adquiridos en la política de gestión,
- Requisitos legales y otros requisitos,
- Opinión de las partes interesadas,
- Aspectos ambientales significativos,
- Opciones tecnológicas, requisitos financieros, operacionales y de negocio que pueden dar lugar a mejoras en la calidad del servicio prestado, en la seguridad de los sistemas de información y en la gestión medioambiental de la organización.

Los objetivos y metas, siempre que sea posible, se cuantifican y refieren a indicadores que permitan evaluar su cumplimiento.

Los objetivos y metas se definen mediante el establecimiento de:

- Plazo de ejecución,
- Situación de partida,
- Situación final,
- Metas y actuaciones para la consecución de los objetivos y las metas, respectivamente,
- Actuaciones necesarias, en su caso, para la definición de las metas
- Frecuencia de seguimiento,
- Responsables de la ejecución.

NOTA: Los objetivos de la gestión de servicios serán desarrollados en el Plan de gestión del servicio correspondiente.
El Responsable del SIG realiza el seguimiento del grado de cumplimiento de cada objetivo y de las metas establecidas a través del seguimiento del programa de gestión.

2.2 Establecimiento y seguimiento del programa de gestión de objetivos

Una vez definidos los objetivos y metas, el Responsable del SGSI elabora el Programa de Gestión de Objetivos que es aprobado por el Director General y distribuido a través de la Intranet de la empresa.

En el citado Programa de Gestión se contempla lo siguiente:

- Objetivo
- Meta
- Indicador asociado (cuando corresponda)
- Actuaciones concretas a llevar a cabo para la consecución de los objetivos y metas propuestos
- Los recursos que serán empleados
- Responsable(s) de la ejecución de las acciones propuestas y los medios (cuando corresponda)
- Fecha de inicio de cada acción concreta
- Fecha de fin prevista para cada actuación concreta
- Fecha de seguimiento para cada actuación
- Resultado del seguimiento de la acción
- Registro o documento relacionado (cuando corresponda)

- Fecha real de fin, es decir, cuando se cerró realmente esa acción propuesta (esta fecha en ocasiones puede ser diferente a la fecha prevista propuesta)

El Responsable del SGSI informa al Comité de Gestión, a través de las reuniones periódicas, de los resultados del seguimiento del programa de gestión y de su grado de avance. Puede promover, a la vista de los resultados del seguimiento del programa de gestión, las acciones preventivas que considere adecuadas, según las directrices del procedimiento convenido.

Si una vez cumplido el plazo para la consecución de alguna acción concreta, ésta no se ha llevado a cabo impidiendo así el cumplimiento de los objetivos y metas establecidos, el Responsable del SGSI procederá con las acciones que considere pertinentes.

Sub-Cláusula 7.2. Competencia

7.2. Competencia

DOCUMENTACIÓN PROPUESTA

OBJETO

Establecer el modo de prever, detectar y satisfacer las necesidades de formación y adiestramiento para cada puesto de trabajo así como evaluar la eficacia de las acciones formativas emprendidas. De igual modo, es objeto de este procedimiento que todos los empleados de LA ORGANIZACIÓN estén debidamente formados y concienciados en material de Seguridad de la información.

ALCANCE

Es de aplicación a todos los empleados de la Organización

DOCUMENTACIÓN DE REFERENCIA

- Norma *ISO/IEC 27001:2013*

ÍNDICE

1. GENERALIDADES

En el contexto de la documentación del SGSI, y en particular, de este procedimiento, se utilizan las siguientes definiciones:

Formación: actividad de enseñar los conocimientos generales y específicos que una persona necesita para desarrollar las actividades asociadas a un determinado puesto de trabajo.

Adiestramiento: actividad de enseñar las habilidades que una persona necesita para desarrollar su labor en un determinado puesto de trabajo. Tiene carácter eminentemente práctico y se relaciona directamente con la tecnología, útiles, equipo, etc., que se utilizan en el puesto de trabajo.

Sensibilización: actividad mediante la que se transmite la pertinencia e importancia de las actividades desarrolladas y de cómo éstas contribuyen a los objetivos generales de LA ORGANIZACIÓN.

2. PROCEDIMIENTO

2.1 Perfiles de Puesto de Trabajo

Para cada puesto de trabajo se define, con la colaboración que se precise de los responsables de departamento de **LA ORGANIZACIÓN**, los requisitos de formación, experiencia y adiestramiento que deben reunir las personas que los ocupen. Dichas características se encuentran definidas en los puestos de trabajo dados de alta en el sistema informático. Se consultarán para creación de ofertas de empleo por el departamento de RRHH.

Para la definición del puesto, el Departamento de Personal define, junto a los responsables de Departamento, y la Dirección General lo siguiente:

1. Tareas del puesto de trabajo
2. Responsabilidades del puesto de trabajo
3. Formación requerida y deseable
4. Experiencia necesaria y deseable
5. Competencias necesarias y deseables
6. Dependencias del puesto

2.2 Ficha del Trabajador

El Responsable del Departamento de Personal mantiene un expediente del trabajador en el que incluye la ficha del trabajador que es rellenada por el trabajador a la firma del precontrato, los informes de actividad formativa y las copias de los títulos y certificados obtenidos en los cursos internos y/o externos.

Además en el sistema informático se creará una ficha para cada empleado en la que se asignará el/los puestos que ocupa pudiéndose adjuntar CV y otros registros de formación.

Desde el sistema informático, cuando un empleado es evaluado o formado, adquiere las competencias y formación correspondientes, que serán indicadas en la ficha del trabajador.

2.3 Detección y planificación de las necesidades de formación

El personal adscrito a un determinado puesto de trabajo es evaluado a intervalos planificados, en cuanto a su formación y adiestramiento, por su responsable directo, por el departamento de RRHH y si procede, por la Dirección General.

Además se realizarán evaluaciones puntuales de la formación y competencias de cada empleado cuando:

- Se modifiquen sensiblemente los métodos de trabajo, los servicios, los procesos o el desarrollo de actividades del sistema integrado de gestión,
- Se pretenda a una persona a otro puesto de trabajo cuyo perfil difiera sensiblemente del puesto que desempeñaba.

El departamento de Personal, a comienzos de año, consulta con los responsables de los distintos departamentos las necesidades de formación detectadas para el personal a su cargo.

RRHH analiza las propuestas realizadas por los responsables de área y las tiene en cuenta para la elaboración del plan de formación anual. Las acciones formativas propuestas pueden incluir tanto actividades de formación teórica (cursos y seminarios) como de entrenamiento práctico y pueden ser a nivel

interno (impartidas por el propio personal del LA ORGANIZACIÓN) o a nivel externo (impartido por empresas de formación externas).

Una vez analizadas las actividades de formación propuestas, el Departamento de RRHH elabora el plan de formación anual identificando las fechas y entidades previstas (proveedor) para la impartición de dichas actividades. Ver anexo 1 de este documento.

Además de la formación expuesta, puede llevarse a cabo alguna acción formativa adicional cuando en el transcurso del año se detecten necesidades de formación no prevista pero necesaria para el desempeño de las funciones.

Las propuestas de formación adicionales se comunican al Departamento de RRHH para que, si el Director General las estima oportunas, se elabore una nueva edición del plan de formación anual.

Siempre que tengan lugar cambios en las normas de referencia del sistema integrado de gestión (ISO 9001, ISO 14001, ISO 27001 y/o ISO 20001) el Responsable del Sistema Integrado de Gestión deberá ser formado en consecuencia para asegurar que los cambios de norma son implementados correctamente en el sistema de gestión.

2.4 Sensibilización

Anualmente se lanzan campañas de sensibilización para todo el personal. Las campañas podrán ser emitidas bien por el departamento de Calidad (Rble. SGSI) o bien por el departamento de RRHH.

La sensibilización incluye, entre otros:

- Importancia del cumplimiento de Políticas y documentación del sistema
- Sensibilización ambiental dirigida al control de aspectos ambientales significativos (consumo de agua, luz, etc.).
- Seguridad de la información
- Protección de datos. Confidencialidad
- Uso de equipos informáticos y otros dispositivos propiedad de la empresa
- Concienciación Servicios al cliente. SLA´s

Una campaña de sensibilización podrá ser un email enviado a todo el personal, cursos presenciales, entrega de documentación, carteles en zonas comunes, etc.

2.5 Empleados de nuevo ingreso

Al su ingreso el empleado recibe el manual de conducta y un manual de bienvenida que incluye una carta de acceso al portal del empleado, donde se encuentran disponibles estos documentos además de las políticas de la Organización y otra documentación relevante.

2.6 Seguimiento de la formación

El Responsable del Departamento de RRHH coordina las acciones necesarias para lograr el cumplimiento de la formación prevista en el plan de formación.

Asimismo verifica que las actividades de formación y adiestramiento se llevan a cabo para lo que entrega a los asistentes al curso/seminario/entrenamiento un informe de actividad de formación a fin de que se lo devuelvan cumplimentado.

El Responsable del Departamento de Personal evalúa la efectividad de las actividades de formación/adiestramiento impartidas mediante:

- Revisión de los informes de actividad de formación
- Revisión de los informes de evaluación de eficacia de la formación

Al final de cada año, el Responsable del Departamento de RRHH realiza una valoración de las actividades formativas desarrolladas, mediante revisión de los registros correspondientes. En ese momento, elabora un informe con las conclusiones de la valoración que presenta al Director General para su estudio y consideración en la revisión anual del Sistema Integrado de Gestión.

2.7 Evaluación de la eficacia de la formación

Para evaluar la eficacia de la formación recibida por los empleados correspondientes, el departamento de RRHH envía la encuesta de impacto de la formación a los responsables del departamento al que pertenece el empleado que ha sido formado, siempre con el objetivo de obtener la confirmación de que la formación realizada ha sido eficaz para el trabajador.

Sub-cláusula 8.1. Planificación y control operacional

8.1. Planificación y control operacional

DOCUMENTACIÓN PROPUESTA

OBJETO

Planificar, implementar y controlar los procesos necesarios en LA ORGANIZACIÓN para cumplir los requisitos de seguridad de la información e implementar las acciones para tratar los riesgos y oportunidades. Así como implementar planes para alcanzar los objetivos de seguridad de la información definidos por LA ORGANIZACIÓN.

ALCANCE

Personal y Sistemas de información del LA ORGANIZACIÓN.

DOCUMENTACIÓN DE REFERENCIA

Norma ISO/IEC 27001:2013

ÍNDICE

1. GENERALIDADES

Es necesario establecer los requisitos de seguridad en las fases de análisis así como las medidas de seguridad oportunas para que el procesamiento de la información se haga sin pérdidas de confidencialidad, integridad o disponibilidad.

Para asegurar que los sistemas de información dan respuesta a las necesidades del LA ORGANIZACIÓN, en lo que respecta a la capacidad, es necesario realizar lo siguiente:

- establecer criterios de aceptación de los sistemas.
- establecer un método que asegure la planificación de la capacidad.
- establecer un método que asegure evaluación de la capacidad.
- definir unos objetivos de mejora.
- trazar un plan de acción (plan de adquisiciones).

2. PROCEDIMIENTO

2.1 Establecer los requisitos de la organización

Se propone tener en cuenta siempre los siguientes requisitos:

- Control de acceso a las aplicaciones (si no es información pública). Como mínimo, se considera el acceso mediante usuario y contraseña para los usuarios.
- Especificación de roles de usuario en función de la naturaleza de la aplicación y la información tratada.
- Incorporación de un log para registrar las acciones críticas. Este log contendrá, como mínimo, los intentos de acceso a la aplicación.
- Seguridad para el tratamiento de documentos, especialmente de carga, copia y descarga de archivos.
- Seguridad en la entrada de datos. Tipos obligatorios. Control de entrada de los datos.
- Seguridad en los enlaces y escalada de privilegios.
- Seguridad en la salida de información. Mínimos privilegios para la obtención de la información.
- Validación de los requisitos del proyecto mediante una fase de pruebas:
    - Validación de los datos de entrada:

        - Los datos introducidos en la aplicación deben validarse antes de pasar a otras partes del sistema, por ejemplo, base de datos.
        - Los campos destinados a la contraseña deberán contener su valor codificado.
    - Utilización correcta de los controles de cifrado, en el caso de que se utilicen.
    - Control de procesamiento interno:
        - Comprobar los datos introducidos para evitar códigos no permitidos o archivos no deseados (en la subida de archivos).
        - Los datos se preparan para su almacenamiento en base de datos sin pérdida de información (utilización correcta de los tipos de datos).
    - Integridad de los mensajes:
        - Los mensajes de error mostrados deben ser concisos y adecuados al error que se produce, no revelando información adicional que permita al usuario conocer la arquitectura de la aplicación (rutas de carpetas o códigos de error del servidor Web, por ejemplo).
    - Validación de los datos de salida:
        - Comprobar que se ha instaurado una política de mínimo privilegio para mostrar la información, dependiendo del perfil del usuario logado.
        - Comprobar que la información mostrada por pantalla corresponde a la información esperada.

2.2 Establecer los requisitos específicos respecto a seguridad de la información

LA ORGANIZACIÓN ha definido los siguientes requisitos que debería cumplir un sistema de información antes de ser adquirido y puesto en producción:

- Calidad y seguridad contrastada en el mercado.
- Soporte por parte del fabricante o distribuidor.
- Satisfacción de las necesidades detectadas.
- Documentación del sistema.
- Compatibilidad con sistemas existentes.
- Resultados de posibles pruebas de puesta en producción (si es posible).
- Facilidad de uso e interfaz amigable (si es HW o SW).

- Relación Calidad / Precio de la aplicación.

2.3 Planificación, implementación y control de procesos

Para cada nuevo proyecto o actividad que requiera utilización de recursos de la empresa, se deben identificar necesidades de capacidad en función de los requisitos del proyecto.

Antes de ponerlo en producción se debe comprobar que la gestión de capacidad realizada sea eficaz. Para ello deben considerarse los siguientes puntos:

- Evaluaciones de la capacidad en el momento de la puesta en producción, ya que puede diferir de la capacidad que había en el momento de la definición de requisitos.
- Pruebas de sistemas realizadas

Para asegurarnos de la implementación y el control, quedan definidos todos los procesos que se llevarán a cabo en las próximas documentaciones propuestas referentes a las cláusulas 6.1 y 6.2.

2.4 Cambios y No Conformidades

Cualquier persona de LA ORGANIZACIÓN que intervenga en alguno de los procesos, puede detectar en el transcurso de los mismos un cambio no previsto o no conformidad aunque normalmente se detectan en alguna de las siguientes operaciones:

- Auditorías del Sistema Integrado de Gestión (externas/internas)
- Reclamaciones recibidas.
- Recepción e inspección de piezas en almacén
- Control de los procesos internos

Se deben diferenciar entre varios tipos de cambio o no conformidad en función de su origen para, a su vez, diferenciar entre varios tipos de tratamientos.

Las posibles decisiones a tomar con respecto a los elementos no conformes son las siguientes:

- Aceptar como está: Decisión de utilizar el elemento no conforme sin modificar ni reparar.
- Rechazar: No es posible modificar o reparar el elemento no conforme.
- Reparar: Modificar el elemento no conforme para convertirlo en conforme con los requisitos modificados.

2.5 Control y Registro de Cambios y No Conformidades

El control y registro de las no conformidades detectadas corresponde al responsable del SGSI. El Responsable del SGSI mantiene actualizado el listado de control en el que queda registrado la fecha y el número/código de No conformidad. Además el Responsable del SGSI incluye en el registro la siguiente información:

- Código: Se deberá indicar el código de siempre que se disponga de él. Por ejemplo, código de C (Cambio) o NC (no conformidad) de auditoría externa.
- Número de C o NC: Las C o NC siguen un orden correlativo. Se otorgará un número a cada C o NC con la siguiente estructura: XX-YY, donde XX son las dos últimas cifras del año vigente e YY es un número correlativo comenzando por el 01 en adelante. Cada año se comenzará una nueva numeración para el caso del valor de YY.
- Fecha C o NC: Siempre se deberá indicar la fecha de apertura del C o NC.
- Lugar de detección: En este campo se debe indicar dónde fue detectado el C o NC (por ejemplo: auditoría interna, auditoría externa, etc.)
- Descripción C o NC: se anotará una descripción detallada del C o NC.
- Tipo: se debe especificar “mayor” o “menor” según corresponda.
- Acciones inmediatas. Se incluirán las acciones inmediatas a tomar para poner fin a la C o NC detectada.
- AC - Acción Correctiva: No todos los C o NC requieren AC puesto que en ocasiones con las acciones inmediatas tomadas es suficiente para ponerla fin. Se debe indicar “Sí” o “No”, según corresponda.
- Código AC/AP: Indicaremos el Código de AC o AP correspondiente, que tendrá la siguiente estructura: AC/XX o AP/XX (En donde: AC indica AC y XX son las dos últimas cifras del año vigente).

NOTA: Cuando no corresponda la apertura de AC se indicará en esta casilla el texto “No Aplica”.

2.6 Definición, registro y seguimiento de acciones correctivas y preventivas

De modo general, las acciones correctivas o preventivas son definidas por el Responsable del SGSI y el personal implicado o por quien aquel determine. Cuando se toma la decisión de establecer una acción correctiva/preventiva el Responsable del SGSI cumplimenta los apartados correspondientes del registro correspondiente.

La dirección General revisa a final de año, en la revisión por la dirección, las acciones correctivas tomadas. El responsable del SGSI completa en el registro la información correspondiente a la AC tomada:

- Tipo de acción: Deberá indicarse si es acción correctiva (AC) o acción preventiva (AP).
- Afecta a: Deberá indicarse a qué parte del SIG afecta (gestión ambiental, calidad, gestión del servicio o seguridad de la información).
- Fecha AC/AP: Deberá indicarse la fecha de planificación de la acción.
- Análisis de las causas: Se indicará el resultado del análisis de las causas realizado, resumiendo la/s causa/s raíz del cambio o NC real para las AC y la causa potencial para las AP.
- Acciones a tomar: Se describirán las acciones a tomar para la eliminación de las causas de la no conformidad detectadas indicando acción, responsable de ejecución de la acción y plazos.
- Estado: Se indicará el estado actual, pudiendo ser: “Abierta” o “Cerrada”.
- Fecha de cierre: Cuando corresponda, se anotará la fecha de finalización de las acciones propuestas, y por tanto, de cierre de la no conformidad.
- Eficacia: Se indicará si las acciones propuestas para poner fin a las causas de las nc y/o nc potenciales han sido eficaces. Marcar con “Sí” o “no”.
- Evidencias: Se indicará un hipervínculo a un correo electrónico y/u otro documento ubicado en la carpeta correspondiente de la AC/AP.
- Comentarios: Se anotarán todos los comentarios que se consideren relevantes para la NC/AC/AP

El estado de la implantación y la eficacia de las acciones correctivas y preventivas definidas serán tratadas en las reuniones por la Dirección celebradas periódicamente.

Sub-cláusula 9.1. Seguimiento, medición, análisis y evaluación

9.1. Seguimiento, medición, análisis y evaluación

DOCUMENTACIÓN PROPUESTA

OBJETO

Describir el procedimiento para mantener en perfecto estado los sistemas de información de LA ORGANIZACIÓN. Revisar el buen desempeño de los sistemas de información de LA ORGANIZACIÓN e identificar posibles sucesos que puedan comprometer la seguridad de la información de la compañía.

ALCANCE

Este procedimiento es de aplicación a los activos del sistema de información de LA ORGANIZACIÓN.

DOCUMENTACIÓN DE REFERENCIA

- Norma *ISO/IEC 27001:2013*

ÍNDICE

1) Generalidades

LA ORGANIZACIÓN empleará la herramienta que considere oportuna (a partir de ahora LA HERRAMIENTA) para la monitorización de los sistemas informáticos. Esta herramienta configurará con un sistema de alertas que lanzan avisos cuando alguno de los elementos monitorizados muestra incidencia.

LA ORGANIZACIÓN además realiza un mantenimiento preventivo en sus máquinas con las siguientes herramientas:

- Desfragmentación de los discos duros (DEFRAQ)
- Escaneado de los discos duros en busca de fallos (SCANDISK)
- Limpieza de temporales (CCLEANER)
- Limpieza del registro (CCLEANER)
- Protección de nuestras máquinas (Firewall de windows)
- Protección anti troyanos, virus, malware y demás (ANTIVIRUS)

Gracias al sistema de la herramienta escogida, se detectarán las alertas en tiempo real y se solucionan en el momento del problema, ya sean sobremesas, portátiles, servidores, impresoras o routers.

En cuanto al mantenimiento preventivo, se harán revisiones de los sistemas según lo especificado en los siguientes puntos. Para cada sistema se establece una frecuencia de revisión diferente según la criticidad del sistema en el Sistema de Información

2) Procedimiento

2.1 Seguimiento

Se especifica por escrito:

- La periodicidad con la que se llevan a cabo el seguimiento y medición
- Quien será el responsable de este seguimiento y medición
- Quien será el responsable de analizar, evaluar e interpretar esos resultados

2.2 Mantenimiento Preventivo

En el anexo 1 se adjunta una tabla con el listado de tareas a realizar, tanto Hardware como Software.

2.3 Mantenimiento Correctivo

Es llevado a cabo conforme a lo descrito en los procedimientos de gestión de incidencias y gestión de peticiones.

2.4 Mantenimiento ERP

2.4.1 Recepción de requerimientos / incidencias

Los requerimientos de cambios o incidencias del ERP utilizado se informan a través de:

- Reuniones de coordinación semanales de las distintas áreas de LA ORGANIZACIÓN en las que se invita al responsable de sistemas para que opine o sugiera la resolución de algún problema de gestión u operativo.
- Correo electrónico enviado por los usuarios al responsable de sistemas reportando alguna sugerencia de cambio o un problema específico

2.4.2 Priorización y selección de requerimientos

Cada quince días se hace un resumen de los requerimientos pendientes y en reunión con la dirección se define las prioridades para cada uno según las necesidades de la empresa.

La selección de requerimientos a desarrollar la hace el responsable de sistemas teniendo en cuenta la prioridad y relación que existe en ellos tanto funcional como técnica.

La propuesta de desarrollo se concreta en un documento al cual asignamos un correlativo y una descripción. Este documento detalla para cada requerimiento la solución que se aplicara en lenguaje funcional, se presenta a la dirección y los usuarios a quienes afectan los cambios para su aprobación u observación.

Una vez aprobada la descripción funcional, se desarrolla la descripción técnica para cada requerimiento, es posible que al detallar los aspectos técnicos se requiera hacer algún cambio en la descripción funcional la que se coordina con los usuarios a quienes pueda afectar para asegurar la viabilidad del cambio.

2.4.3 Desarrollo de un documento de requerimientos (RQ)

Dependiendo de la complejidad de las modificaciones a realizar se asignan los desarrollos al personal técnico correspondiente y se hace un seguimiento semanal para ver avances y posibles distorsiones de las fechas prometidas de entrega a la dirección de LA ORGANIZACIÓN.

Una vez terminados los desarrollos se prepara una base de datos de prueba en la que aplicaran los cambios realizados haciéndose las validaciones correspondientes para asegurar que el resultado es el buscado, si las pruebas no resultan correctas se hacen las observaciones del caso y vuelve al proceso de desarrollo para corregir lo que corresponda, de lo contrario, se coordina con el o los usuarios correspondientes para que validen los cambios efectuados buscando su aprobación para la implantación en la base de datos de producción.

2.4.4 *Implantación* de desarrollos (RQ)

Al montar los cambios en la base de datos en producción se aplican los requerimientos previos de datos, configuraciones y definición de parámetros.

A continuación se forma a los usuarios que requieran y se establece un periodo de atención prioritaria para resolver dudas, posibles errores o por si se presentaran problemas no previstos en otras áreas o módulos del sistema.

2.4.5 *Aceptación* del cambio

El departamento de desarrollo comunicará al solicitante del requerimiento la puesta en marcha de su requerimiento con la finalidad de que realice las comprobaciones pertinentes. Se entiende que el cambio realizado es correcto, si el usuario no responde el mail enviado en el plazo de una semana.

2.5 Monitorización

Con el objeto de asegurar el buen desempeño de los sistemas de información de LA ORGANIZACIÓN e identificar posibles sucesos que puedan comprometer la seguridad de la información y gestión de los servicios ofrecidos por la compañía se ha implanta LA HERRAMIENTA.

La monitorización es responsabilidad del Departamento de Sistemas Internos. Los activos que se han monitorizado se anexan en el anexo 2 de este documento. Los datos serán recolectados mediante LA HERRAMIENTA y almacenados en una base de datos MYSQL.

Toda monitorización deberá llevar asociada la definición de umbrales para la generación de avisos y/o alarmas. Por defecto los umbrales para las máquinas más críticas son los siguientes:

1) Para capacidad en los discos 10% libre WARNING y 5% libre CRÍTICO.
2) Para el uso de memoria 20% libre WARNING y al 10% libre CRÍTICO.
3) Para el uso de CPU 15% usado WARNING y al 30% usado CRÍTICO.

Para una ágil interpretación de los resultados de la monitorización, se establece un código de colores que facilita la comprensión visual. Los colores indican lo siguiente:

- Rojo: Incidencia crítica. Requiere de una inmediata actuación por parte del responsable de Soporte. Se ha definido como incidencia crítica cuando están logados más de 5 usuarios.
- Amarillo: Incidencia leve. Requiere de asistencia, pero no se corre el riesgo de pérdida de información. Se ha definido como incidencia leve cuando hay logados de 1 a 5 usuarios.
- Verde: Estado correcto.
- Naranja, que significa que la incidencia que estuviese ocurriendo no estaría codificada. Por defecto, este color aparece cuando NAGIOS no es capaz de catalogar el error o incidencia. Lo habitual es que, una vez definido el servicio, no aparezca este color.

Pueden existir otros chequeos dependiendo del servidor y pueden existir servidores con umbrales específicos más restrictivos, debido a necesidades del servicio.

Se harán evaluaciones cada 6 meses y se crearán los correspondientes informes, extrayendo las conclusiones oportunas, que podrán ser utilizados para la gestión de capacidad de los sistemas de información de la empresa.

3) ANEXOS

3.1 Mantenimiento Preventivo

HARDWARE		
TAREAS	**CONSIDERACIONES**	**PERIODICIDAD**
SERVIDORES		
Limpieza física de la máquina	Revisión en equipos con ubicaciones con más probabilidades de contaminación	Trimestral
PORTATILES		
Limpieza física de la máquina	Revisión en equipo con ubicaciones con más probabilidades de contaminación	Trimestral
SOBREMESAS		
Limpieza física de la máquina	Revisión en equipo con ubicaciones con más probabilidades de contaminación	Semestral
IMPRESORAS		
limpieza de rodillos, cabezales y otras piezas mecánicas	En caso de atascos o problemas de impresión	Semestral
Rutinas de diagnóstico de la impresora	Revisión de la Web de las impresoras de Red. Verificar tóner o tinta. Consumo total de papel	Semestral
FAX		
Limpieza de rodillos	En caso de atascos o problemas de impresión. Verificación de tóner o tinta	Semestral
SOFTWARE		
TAREAS	**CONSIDERACIÓNES**	**PERIODICIDAD**
SERVIDORES		
Mantenimiento y actualización del antivirus, spyware y firewall	El antivirus/spyware se actualiza diariamente. El FW de Windows se deja configurado desde el inicio	Trimestral
desfragmentación y scandisk de los discos duros	se revisa/ejecuta cuando se nota lentitud en el sistema	Trimestral

Backup	Diario Incremental / Completo Semanal	Diario/semanal
Limpieza de registro (registros obsoletos)	Se revisa ejecuta cuando se nota lentitud en el sistema	Trimestral
Revisión de actualizaciones del sistema operativo	Se revisa todo cada 15 días, o cuando se recibe alguna alerta de las listas de seguridad	Quincenal
Revisión del visor de eventos en todas sus categorías.		Mensual
PORTÁTILES		
Mantenimiento y actualización del antivirus, spyware y firewall	El antivirus/spyware se actualiza diariamente. El FW de Windows se deja configurado desde el inicio	Semestral
desfragmentación y scandisk de los discos duros	se revisa/ejecuta cuando se nota lentitud en el sistema	Semestral
Limpieza de registro (registros obsoletos)	Se revisa ejecuta cuando se nota lentitud en el sistema	Semestral
Revisión de actualizaciones del sistema operativo	Cuando se recibe alguna alerta de las listas de seguridad	Trimestral
Revisión del visor de eventos en todas sus categorías.		Mensual
PC SOBREMESA		
Mantenimiento y actualización del antivirus, spyware y firewall	El antivirus/spyware se actualiza diariamente. El FW de Windows se deja configurado desde el inicio	Semestral
Desfragmentación y scandisk de los discos duros	se revisa/ejecuta cuando se nota lentitud en el sistema	Semestral

Limpieza de registro (registros obsoletos)	Se revisa ejecuta cuando se nota lentitud en el sistema	Semestral
Revisión de actualizaciones del sistema operativo	Cuando se recibe alguna alerta de las listas de seguridad	Trimestral
Revisión del visor de eventos en todas sus categorías.		Mensual

3.2 Activos Monitorizados

SERVIDORES WINDOWS

- Nombre del servidor [Dirección IP]

ROUTERS INTERNOS

- Nombre dado al router [Dirección IP]

Sub-cláusula 9.2. Auditoría interna

9.2. Auditoría interna

DOCUMENTACIÓN PROPUESTA

OBJETO

Definir la metodología empleada por el LA ORGANIZACIÓN para llevar a cabo las auditorías internas de su Sistema Integrado de Gestión con el fin de verificar que se ha implantado y que es eficaz o, en caso contrario, para detectar las anomalías y establecer las acciones correctivas necesarias para eliminarlas.

ALCANCE

Este Procedimiento es de aplicación a todos los procesos y recursos de COS.

DOCUMENTACIÓN DE REFERENCIA

- Norma *ISO/IEC 27001:2013*

ÍNDICE

1. Generalidades

En el contexto de la documentación del Sistema Integrado de Gestión, y en particular, de este procedimiento, se utilizan las siguientes definiciones:

Auditoría del Sistema Integrado de Gestión: proceso de verificación sistemático, independiente y documentado para obtener y evaluar objetivamente evidencias de auditoría para determinar si el Sistema Integrado de Gestión del LA ORGANIZACIÓN se ajusta a los criterios de auditoría del Sistema Integrado de Gestión y para la comunicación de los resultados a la Dirección General.

Auditor: persona cualificada para realizar las auditorías.

Auditor jefe: persona designada cuando la auditoría la realiza un equipo para ser responsable de organizar y dirigir la misma, informar sobre las evidencias encontradas, valorar estas evidencias y de elaborar y firmar el informe de auditoría, todo ello asegurando objetividad e imparcialidad.

Equipo Auditor: grupo de auditores, con un auditor jefe responsable, designado para efectuar la evaluación de la calidad. A este equipo se podrá unir uno o más observador

Auditado: Responsable de un área que va a ser sometido a control por parte del auditor para comprobar el cumplimiento del área a su cargo respecto del marco normativo de referencia.

Evidencia de auditoría: información verificable, registros, declaraciones de hecho o cualquier otra información que son pertinentes para los criterios de auditoría.

Criterios de auditoría: conjunto de políticas, prácticas, procedimientos o requisitos en relación a los que el auditor compara las evidencias de auditoría recogidas sobre el objeto de ésta.

Hallazgo de auditoría: resultados de la evaluación de las evidencias de auditoría recogidas y comparadas con los criterios de auditoría acordados.

Informe de auditoría: documento donde se detallan los resultados obtenidos durante el proceso de auditoría

2. Procedimiento

2.1 Planificación

A principios de cada año, el Responsable del Sistema Integrado de Gestión (en adelante Responsable del SGSI) elabora el programa anual de auditoría interna. La planificación de las auditorías internas tiene en cuenta el estado e importancia de los procesos/actividades que van a auditarse, y el resultado de auditorías previas.

El Responsable del SGSI documenta la programación anual en el programa de auditorías internas en el que recoge los departamentos que deben auditarse, las fechas previstas para ello y los auditores propuestos. También puede cumplimentar una lista de comprobación para cada departamento que vaya a auditarse recogiendo las actividades y funciones a auditar.

El Responsable del SGSI mantendrá actualizado un listado con la relación de auditores internos que estarán autorizados por LA ORGANIZACIÓN para realizar auditorías internas, indicando la/las norma/s que puede auditar cada auditor.

El Responsable del SGSI envía el borrador del programa de auditorías internas a los responsables afectados que pueden proponer modificaciones en cuanto a las fechas previstas.

Una vez incluidas las modificaciones propuestas, el programa de auditorías internas es aprobado por la Dirección General.
Una vez aprobado, el Responsable del SGSI archiva el programa de auditorías internas y remite copias del mismo al personal del LA ORGANIZACIÓN implicado en dicho programa.

Además de las auditorías incluidas en el programa de auditorías internas, pueden realizarse otras auditorías cuando:

- Se hayan introducido modificaciones significativas en el Sistema Integrado de Gestión,
- Se sospeche o se tenga la certeza de que el nivel de calidad, gestión ambiental, seguridad de la información o gestión de servicios TI está comprometido
- Se deba verificar la implantación de acciones correctivas

Si durante la vigencia del programa de auditorías internas se considera conveniente incluir alguna de las auditorías extraordinarias citadas u otras causas se modificará la programación y se emitirá una nueva edición del programa de auditorías internas de modo similar a lo descrito para el programa de auditorías internas original.

2.2 Cualificación de auditores

La realización de las auditorías internas es llevada a cabo por personal del LA ORGANIZACIÓN calificado como auditor o por auditores externos de entidades que acrediten de manera previa a la realización de la auditoría, lo siguiente:

- Disponer de la norma ISO/IEC 27001:2005.
- Disponer de procedimientos para la realización de auditorías de sistemas de gestión.
- Estar cualificado de acuerdo a procedimientos internos de la empresa. La calificación como auditor para el personal del LA ORGANIZACIÓN consiste en:
    - Entendimiento íntegro de la norma *ISO/IEC 27001:2013*.
    - El conocimiento de las auditorías internas de los sistemas de gestión según *ISO/IEC 27001:2013*.
    - Garantía y compromiso de objetividad e imparcialidad.
    - Muy recomendable conocimientos o experiencia previa en auditorías internas.

2.3 Asignación de los auditores

Las auditorías pueden ser realizadas por un único auditor o un equipo auditor compuesto por un auditor jefe y un número de auditores variable en función de la envergadura de la auditoría.

Tanto si las auditorías son realizadas por personal interno del LA ORGANIZACIÓN como si son realizadas por personal externo, la asignación de cada auditoría (aprobación de la propuesta de constitución del equipo auditor) la lleva a cabo la Dirección General mediante la aprobación del programa de auditorías internas.

El personal de LA ORGANIZACIÓN que participe en la realización de auditorías internas debe ser independiente de la actividad que audite.

2.4 Preparación de la auditoría

El auditor o equipo auditor, con la colaboración del Responsable del SGSI revisa y prepara la documentación necesaria para llevar a cabo la auditoría, incluidas, en su caso, las listas de comprobación.

Las bases para preparar la auditoria serán la documentación del Sistema Integrado de Gestión de LA ORGANIZACIÓN, el informe de la auditoría precedente, la Norma *ISO/IEC 27001:2013*, así como cualquier otra normativa o reglamentación aplicable.

El Responsable del SGSI recuerda al responsable del departamento que va a ser auditado, como mínimo con diez días de antelación a la fecha de la auditoría, el alcance de la misma y las verificaciones que se van a llevar a cabo la realización de la auditoría.

La auditoría se lleva a cabo en las fechas previstas en el programa de auditorías internas y se realiza de modo presencial por el auditor o equipo auditor designado, que recaba la presencia del responsable de la actividad o función que se va a auditar para que facilite las evidencias objetivas y datos necesarios solicitados para el cumplimiento satisfactorio de la actividad dentro del alcance fijado.

La auditoría comienza con una breve reunión inicial en la que el auditor comenta con los responsables implicados las verificaciones que van a llevarse a cabo.

Las verificaciones a efectuar durante la auditoría son, en general, de la siguiente naturaleza:

- Revisión de los documentos del Sistema Integrado de Gestión utilizados: se comprueba que cada Dirección/Departamento de LA ORGANIZACIÓN dispone de los documentos del Sistema Integrado de Gestión que le son aplicables así como que los responsables correspondientes emiten, distribuyen y controlan adecuadamente los documentos a su cargo.

- Examen de los registros de datos generados y evidencias documentales que demuestren el cumplimiento de los requisitos del Sistema Integrado de Gestión, incluidos aspectos relativos a formatos utilizados, sistema de archivo, destino, etc.

- Supervisión directa de las actividades que se realizan para comprobar que cada una de las actividades encomendadas para la realización de los trabajos se están desarrollando de la manera prescrita en la documentación del Sistema Integrado de Gestión.

En el desarrollo de la auditoría, el auditor tiene siempre en cuenta que:

- Se evalúan solamente evidencias objetivas y contrastadas,

- La verificación no tiene por qué limitarse a los aspectos recogidos, en su caso, en la lista de comprobación, en caso de detectarse una posible deficiencia se investigará hasta confirmarla o no, averiguar si es sistemática o fortuita e identificar en lo posible sus efectos y causas

- Se someten a un seguimiento exhaustivo las no conformidades y anomalías detectadas en auditorías anteriores.

Una vez finalizada la auditoría, el auditor o equipo auditor mantiene una reunión con el responsable de la actividad o función auditada y le expone las desviaciones encontradas para obtener su acuerdo con las mismas o para que formule sus observaciones.

2.5 Informe de auditoría

En el plazo de 15 días a partir de la fecha de finalización de la auditoría el auditor elabora el informe de auditoría y es el Responsable del SGSI quien procede a su archivo físico en la carpeta correspondiente.

En el Informe registra, como mínimo, los siguientes datos:

- Criterio/objeto de la auditoría
- Alcance (Dirección/Departamento o actividad a auditar)
- Fecha de la auditoría
- Frecuencia de la auditoría
- Documentación de referencia
- Auditor o equipo auditor
- Descripción de los métodos la auditoría
- Las responsabilidades
- Los requisitos de planificación
- Elaboración de informes que incluyan:

  - Resumen de hallazgos (no c conformidades/observaciones/recomendaciones)
  - Sugerencias de mejora del departamento auditado.

- anexos: se incluyen los que se estimen oportunos para aclarar la información sobre las no conformidades detectadas

El Responsable del SGSI realiza distribuye por correo electrónico una copia del informe de auditoría a los responsables de los departamentos auditados para comunicar los hallazgos encontrados.

2.6 Acciones correctivas derivadas de auditoría

Cuando se detecte una no conformidad en alguna de las auditorías internas realizadas, se deberá proceder a la definición e implantación de una acción correctiva.

El Responsable del SGSI, junto con la dirección general y el responsable del proceso en donde se ha detectado la no conformidad propondrán las acciones correctivas necesarias analizando las causas de las no conformidades.

Posteriormente, es el Responsable del SGSI quién efectúa el seguimiento, cierre y archivo de las acciones correctivas derivadas de las auditorías.

3. ANEXOS

Se propone mantener una documentación que contenga:

- Checklist/comprobación de la auditoría
- Programa de cada auditoría
- Relación de auditores internos
- Conformidad de auditorías

Sub-cláusula 9.3. Revisión por la dirección

9.3. Revisión por la dirección

DOCUMENTACIÓN PROPUESTA

OBJETO

Determinar las directrices para el análisis de los datos y para la revisión del Sistema Integrado de Gestión en lo que respecta a su conveniencia, adecuación y eficacia.

ALCANCE

Este procedimiento es de aplicación al Comité de Gestión como órgano interno que lidera la implantación y mantenimiento del Sistema Integrado de Gestión y al Director General como máximo responsable del mismo.

DOCUMENTACIÓN DE REFERENCIA

- Norma ISO/IEC 27001:2005

ÍNDICE

1. Generalidades

<No Aplica>

2. Procedimiento

El Responsable de Seguridad de la Información (en adelante, Responsable del SGSI) recaba la siguiente información:

- Estado de las Acciones desde la anterior revisión
- Cambios en cuestiones externas e internas que podrían afectar al Sistema Integrado de Gestión
- Desempeño de las no conformidades del producto/servicio
- Estado de las Acciones correctivas y preventivas
- Seguimiento del plan de gestión de los servicios.
- Resultado de las mediciones de eficacia
- Acciones de seguimiento de revisiones previas por la Dirección
- Resultados de las auditorías (internas y externas)
- Cumplimiento de Objetivos del Sistema Integrado de Gestión
- Cumplimiento de Objetivos específicos para la gestión del servicio
- Evaluación del Sistema Integrado de Gestión en su doble aspecto, documentación e implantación por áreas
- Evaluación del cumplimiento legal
- Evaluación de proveedores
- Comunicaciones de las partes interesadas
- Resultado de la apreciación del riesgo
- Estado del plan de tratamiento de riesgos
- Oportunidades de mejora detectadas. En este apartado debe estudiarse la necesidad de efectuar cambios en el Sistema Integrado de Gestión, incluyendo la política de gestión así como en los recursos disponibles
- Recomendaciones para la mejora

El Comité de Gestión se reúne a intervalos planificados para someter a revisión al Sistema Integrado de Gestión. Las revisiones por la Dirección tienen lugar una vez al año.

El Comité de Gestión, evalúa las oportunidades de mejora detectadas y establece las acciones que deben llevarse a cabo para la mejora de la eficacia del Sistema Integrado de Gestión y de las actividades y prestación del

servicio en función de los requisitos del cliente y la provisión de recursos. Como resultado de la revisión por la dirección se tomarán decisiones y acciones relativas a:

- Nuevos objetivos para el plan de gestión del siguiente ciclo
- Nuevos recursos para la gestión del sistema
- Actualización de la valoración de los riesgos y de plan de tratamiento de los mismos
- Modificación de los procedimientos, procesos de gestión y de los controles de seguridad de la información; incluyendo posibles cambios en.
- Requisitos de negocio
- Requisitos de seguridad
- Procesos de negocio
- Requisitos legales
- Obligaciones contractuales
- Niveles de riesgo y/o criterios de aceptación de riesgos
- Mejora en el modo de medir la eficacia (métricas) de los procesos y controles implantados en el Sistema Integrado de Gestión

Igualmente se definen los responsables de dichas acciones y los plazos para su ejecución. Con esta información se recomienda crear un documento de nombre “Plan de mejora del Sistema Integrado de Gestión”
Como resultado de la revisión del sistema, el Responsable del SIG redacta un acta que constituye el informe de revisión a presentar en las auditorías externas del sistema.

El Sistema Integrado de Gestión se revisa una vez al año excepto cuando se produzca alguna de las siguientes situaciones que hagan aconsejable una revisión anticipada:

- Cambio de la política del Sistema Integrado de Gestión,
- cambio de los recursos disponibles,
- Detección de carencias graves a través de las auditorías internas o externas,
- Desarrollo de mejoras representativas en el Sistema Integrado de Gestión.

3. ANEXOS

Se propone mantener una documentación que contenga:

- Plan de mejora del Sistema Integrado de Gestión

CONCLUSIONES

En este trabajo se ha realizado una revisión completa de la norma ISO/IEC 27001:2013, que es un estándar para la seguridad de la información en el que se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información de acuerdo con el Ciclo de Deming: Planificar-Hacer-Comprobar- Actuar (ciclo PDCA)..

Se ha explicado y desglosado la norma ISO/IEC 27001:2013 y los cambios con respecto a la versión anterior ISO/IEC 27001:2005 y se ha propuesto una documentación mínima para llevar a cabo la certificación. . En concreto, se ha desarrolla la documentación para:

- Planificar: política, acciones para tratar los riegos de seguridad, los objetivos de seguridad, competencias,
- Hacer: planificación y control operacional, apreciación de los riesgos de seguridad, tratamiento de los riesgos de seguridad
- Comprobar: Seguimiento y medición, auditoria interna, revisión por la dirección.

Además, se ha hecho un breve recorrido por la historia de la información hasta llegar al momento actual, se ha justificado la necesidad de implantar un Sistema de Gestión de la Seguridad de la Información, así como los beneficios que aporta en una pequeña o mediana empresa.

Aunque la norma ISO/IEC 27001 es aplicable a cualquier organización independientemente de su tamaño o sector, puesto que en todas encontramos volúmenes de información con los que hay que trabajar y sobre los que hay que garantizar cierta seguridad, el sector de las tecnologías de la información (IT - Information Technology) se impone entre los sectores industriales (según los datos internacionales de 2012 de ISO.org), debido a que la certificación es especialmente adecuada cuando la protección de la información es crítica. Se ha efectuado un análisis de Porter del sector IT y telecomunicaciones.

.

BIBLIOGRAFÍA

AENOR (2007) *UNE-ISO/IEC 27001:2007* Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

AENOR (2014) *UNE-ISO/IEC 27001:2014* Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.

Alberts C, Dorofee A (2003) *Managing information Security Risks. The OCTAVE Approach,* Addison Wesley.

Alexander A G (2007) *Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001:2005,* Alfaomega Colombiana.

Bologna G J, Walsh A M (1997) *The Accountant's Handbook of Information Technology,* Wiley.

BSI group. (2013a) *Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013.*

BSI group. (2013b) *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013; The new international standard for information security management systems.*

Burton R. N. (2000) *Discussion of Information Technology-Related Activities of Internal Auditors,* Journal of Information Systems: Supp., Vol. 14, No. s-1, pp. 57-60

Corletti A (2007) *ISO-27001 y las PyMEs,* Revista DINTEL, No. 13, pp. 148-151

Díaz S, Cayón A, Alonso A. (2008) *Código Unión Europea,* La Ley.

ISO (2005) *ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements.*

ISO (2013) *ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.*

ISOTools Excellence. (2014 a) *La Norma ISO 27001 y la importancia de la Gestión de la Seguridad de la Información. Alcanzar la excelencia en la Seguridad de la Información. Un mejor servicio con una menor inversión*.

ISOTools Excellence. (2014 b) *Las claves del Éxito para la Gestión de Riesgos de Seguridad de la Información.*

Landoll D. (2011) *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risks Assesments*, CRC Press.

Linares R, Patterson M, Viciedo L. (1999) *La información a través del tiempo*, Revista ACIMED Vol 8 número 3.

Parra Valbuena A (2009) Modelo de porter y estrategias de negocio de operadores de telecomunicaciones en España. Proyecto Fin de Carrera. Escuela Técnica Superior d'Enginyeria de Telecomunicació de Barcelona. Universidad Politécnica de Catalunya.

Porter E M (2003). Ser competitivo. Nuevas aportaciones y conclusiones. Ediciones Deusto. Barcelona.

San Martín García, J.M. (2004) La seguridad de la información. Legislación Actual de Seguridad de la Información (II/IV), Anales de mecánica y electricidad, Marzo-Abril 2004.

WEBS COSULTADAS

Blog firma-e:
http://blog.firma-e.com
(última visita 17-04-2015)

Blog Clearswift:
http://www.clearswift.com/blog/2013/05/02/enemy-within-emerging-threat
(última visita 02-03-2014)

El portal de ISO 27001 en Español:
http://www.iso27000.es/
(última visita 26/12/2014)

International Organization for Standardization
http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001
(última visita 28/12/2014)

Portal de Administración Electrónica · Ministerio de Hacienda y Administraciones Públicas · Secretaría de Estado de Administraciones Públicas:
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VWLsNU_tmkr
(última visita 08-04-2015)