
Auditoría de la información

PID_00270516

Antonio José Segovia Henares

**Antonio José Segovia Henares**

Ingeniero informático e ingeniero técnico en informática de sistemas. Docente universitario y auditor líder cualificado en diferentes esquemas nacionales e internacionales como el Esquema Nacional de Seguridad, el RGPD y las ISO 27001, ISO 22301 y ISO 20000.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Helena Rifà

Primera edición: marzo 2020
© de esta edición, Fundació Universitat Oberta de Catalunya (FUOC)
Av. Tibidabo, 39-43, 08035 Barcelona
Autoría: Antonio José Segovia Henares
Producción: FUOC
Todos los derechos reservados

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este eléctrico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita del titular de los derechos.

Índice

Introducción.....	5
Objetivos.....	6
1. La auditoría de protección de datos.....	7
1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la auditoría	7
1.1.1. Preauditoría	9
1.1.2. Auditoría	12
1.1.3. Posauditoría	15
1.2. Elaboración del informe de auditoría: aspectos básicos e importancia del informe de auditoría	18
1.3. Ejecución y seguimiento de acciones correctoras	21
2. Auditoría de sistemas de información.....	25
2.1. La función de la auditoría en los sistemas de información. Conceptos básicos. Estándares y directrices de auditoría de seguridad de la información	25
2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de seguridad de la información	29
2.3. Planificación, ejecución y seguimiento	38
3. La gestión de la seguridad de la información.....	40
3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2017): requisitos de sistemas de gestión de seguridad de la información, SGSI)	40
3.2. Gestión de la seguridad de los activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación	48
3.3. Recuperación ante desastres y continuidad del negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la recuperación ante desastres	56
Resumen.....	58
Bibliografía.....	61

Introducción

En este módulo veremos el proceso completo para llevar a cabo una auditoría de protección de datos personales y cuál es la regulación actualmente aplicable. Además, veremos otros estándares internacionales relacionados con la protección de datos y que también se pueden considerar a la hora de llevar a cabo auditorías de la información.

Es importante destacar que cuando hablemos de protección de datos nos referiremos a datos personales, mientras que cuando hablemos de sistemas de información, nos referiremos a los sistemas (generalmente servidores) donde se almacenan digitalmente los datos personales.

Objetivos

Con la lectura de este módulo el estudiante alcanzará los siguientes objetivos:

- 1.** Conocer las características básicas de las auditorías.
- 2.** Conocer las auditorías de protección de datos.
- 3.** Aprender cómo enfocar y elaborar un informe de auditoría.
- 4.** Conocer las acciones correctivas dentro del proceso de auditoría.
- 5.** Conocer las auditorías de sistemas de información.
- 6.** Aprender cómo se integra la auditoría de sistemas de información con las auditorías de protección de datos.
- 7.** Aprender a planificar las auditorías.
- 8.** Saber gestionar la seguridad de la información.

1. La auditoría de protección de datos

Dentro del marco de la protección de datos personales, dado que tenemos que regirnos por una ley específica, como es la **Ley orgánica de protección de datos personales y garantía de los derechos digitales** (LOPD-GDD), es importante conocer el nivel de cumplimiento de esta ley o, mejor dicho, saber si cumplimos o no con ella.

LOPD-GDD

La LOPD-GDD es la actual normativa española relativa a la protección de datos personales, la cual sustituye a la anterior Ley orgánica de protección de datos personales (LOPD).

Generalmente, si hemos llevado a cabo todas las cuestiones necesarias para cumplir con la LOPD-GDD o incluso hemos seguido alguna de las guías publicadas por la Agencia Española de Protección de Datos, podremos pensar que cumplimos con la ley y que no es necesario realizar ninguna auditoría. Sin embargo, esto no tiene por qué ser así, ya que existen muchas interpretaciones y, en este caso, diferentes soluciones para el mismo problema. Además, también puede ocurrir que la interpretación que hagamos esté mal y que ello implique un incumplimiento, lo que puede llegar a significar una sanción económica.

Para evitar esta incertidumbre, lo ideal es que un experto en la materia o un grupo de profesionales, independiente y, a ser posible, ajeno a la organización, revise el cumplimiento de la LOPD-GDD. Cuanto más independiente sea el experto, más objetivo podrá ser, y la revisión podrá ofrecer unos resultados más fiables.

Estas revisiones son las que realmente se llevan a cabo durante un proceso de auditoría y es lo que iremos desarrollando a lo largo de los próximos subapartados. Estos irán enfocados en la protección de datos, aunque el proceso de auditoría en sí mismo es generalmente siempre el mismo.

1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la auditoría

Imaginemos la empresa ficticia Informática y Servicios, S. L., que ha contratado un proveedor especializado en protección de datos personales, y que este, después de ciertas jornadas de trabajo asesorando a la organización, culmina su trabajo confirmando que Informática y Servicios, S. L. ya cumple con la LOPD-GDD.

Para muchos esto ya podría ser suficiente, pero lo ideal es ir un paso más allá: es el momento de iniciar el proceso de auditoría.

Realmente, la LOPD-GDD no establece de manera concreta y específica un requisito que obligue a todas las organizaciones a llevar a cabo estas auditorías, pero, como se ha comentado anteriormente, para evitar incertidumbres es bastante recomendable.

Esta revisión, además, independientemente de lo que diga la LOPD-GDD, tiene mucho sentido, porque, como se suele decir, «cuatro ojos ven más que dos», es decir, no es lo mismo que llevemos a cabo una actividad por nosotros mismos y luego seamos nosotros quien la revisemos a que nosotros la realicemos y otra persona distinta, con otro enfoque diferente, haga la revisión. Los resultados de la revisión realizada por la persona «externa» serán mucho más objetivos y mucho más fiables.

Por otra parte, una de las obligaciones que tiene el **delegado de protección de datos** (DPD) es la supervisión del cumplimiento de la normativa, pero esta supervisión no puede llevarla a cabo él mismo. Si la hiciese él mismo, rompería el principio de imparcialidad y podría representar un incumplimiento con respecto a la normativa.

Otros principios de la LOPD-GDD que debe cumplir la organización y que un auditor debe comprobar que existen son los siguientes:

- **Licitud, transparencia y lealtad:** los datos del interesado deben ser tratados de manera lícita, transparente y leal.
- **Limitación de la finalidad:** los datos del interesado deben ser tratados con una finalidad determinada, que tiene que ser explícita y legítima. Es decir, no está permitido recopilar datos para un fin y tratarlos para otro fin distinto.
- **Minimización de datos:** los datos del interesado deben ser adecuados y limitados a lo estrictamente necesario para los fines para los que son tratados.
- **Principio de exactitud:** los datos del interesado deben ser precisos y exactos y deben estar actualizados.
- **Limitación del plazo de conservación:** los datos del interesado solo se podrán conservar durante el tiempo que sean tratados. Una vez finalizado el tratamiento, serán eliminados.
- **Integridad y confidencialidad:** los datos del interesado deben estar protegidos contra amenazas que puedan afectar a su confidencialidad e integridad.

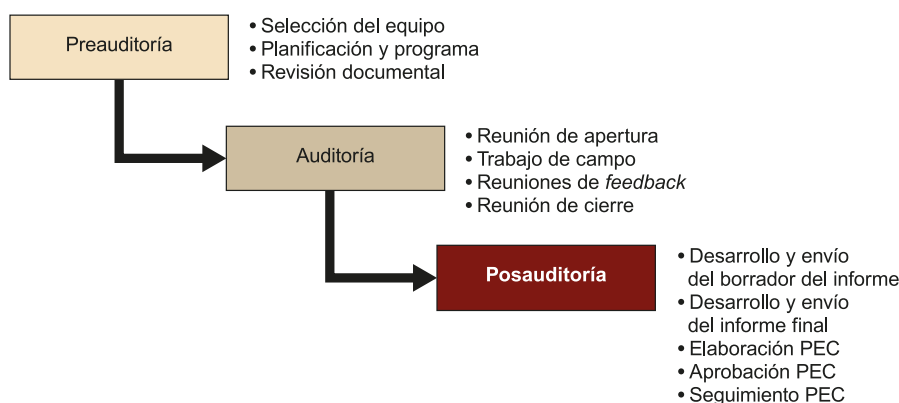
- **Responsabilidad proactiva:** los datos del interesado estarán protegidos con medidas técnicas y organizativas para garantizar y demostrar que el tratamiento de los datos se realiza conforme a la LOPD-GDD.

El DPD puede contratar a un proveedor externo, independiente y especializado para que realice una auditoría de cumplimiento. Sobre la base de los resultados de esta auditoría, el DPD puede supervisar el cumplimiento de la organización con respecto a la LOPD-GDD y puede llegar a determinar que todo está correcto (o no, dependiendo de los resultados de la auditoría).

Como ya hemos comentado, la realización de esta auditoría no es obligatoria. El DPD puede llevar la supervisión del cumplimiento de la normativa como lo estime oportuno, con auditoría o sin ella.

Con respecto al proceso de auditoría en sí, podemos dividirlo principalmente en las etapas que se muestran en la figura 1.

Figura 1. Principales etapas del proceso de auditoría



A continuación, veremos el detalle de cada una de las actividades que componen cada etapa.

1.1.1. Preauditoría

El objetivo de la preauditoría es llevar a cabo los preparativos necesarios para realizar la auditoría.

Las actividades que componen la preauditoría son las siguientes:

1) Selección del equipo. Es importante contar con personal que esté adecuadamente cualificado, no solo en la LOPD-GDD, sino que también tenga formación específica en la realización de auditorías. Un profesional puede cono-

Enlace de interés

Para que veáis la importancia de estas auditorías, a pesar de no ser estrictamente obligatorias, podéis consultar la página web de la Information Commissioner's Office, que podemos decir que es la equivalente británica a la Agencia Española de Protección de Datos Personales, que lleva a cabo auditorías tanto a empresas privadas como públicas para comprobar el nivel de cumplimiento con respecto al GDPR. Estas auditorías actualmente son gratuitas y su resumen ejecutivo es publicado en la página web de esta entidad, desde donde cualquier persona puede tener acceso.

cer a la perfección la normativa, pero si después no sabe cómo llevar a cabo una auditoría, no podrá recopilar la información que necesitamos para comprobar el cumplimiento con respecto a la LOPD-GDD.

Generalmente, los auditores cualificados en estándares ISO, como ISO 27001, ISO 22301, ISO 9001, etc., tienen un conocimiento adecuado del proceso de auditoría porque estas auditorías deben llevarse a cabo de acuerdo a una guía específica, que es la establecida por la ISO 19011 (aunque en el caso concreto de la ISO 27001, existe la guía ISO 27007, que por otra parte es muy similar a la ISO 19011).

Por otro lado, dado que la LOPD-GDD no habla de manera explícita de la realización de auditorías de cumplimiento, es obvio pensar que tampoco establezca requisitos mínimos para el perfil de un auditor que se encargue de comprobar este cumplimiento.

Si el equipo auditor está compuesto por diferentes personas, se debe designar un **auditor jefe** que será quien lidere las actividades relativas al proceso de auditoría y quien mantenga en primera línea el contacto con la empresa que hay que auditar. Este auditor jefe también se suele conocer como auditor líder.

2) Planificación y programa. Una vez seleccionado el equipo auditor y establecida la figura del **auditor líder**, es el momento de planificar la realización de la auditoría. Esta planificación debe ser consensuada entre el equipo auditor y la organización que hay que auditar, y contendrá el detalle de los días y los horarios en los que se llevarán a cabo las visitas.

Generalmente, dos o tres jornadas son suficientes para realizar una auditoría de cumplimiento de la LOPD-GDD, pero este tiempo puede ser incrementado o disminuido dependiendo de la complejidad de la organización.

Por otra parte, si la organización posee diferentes centros, será necesario determinar la necesidad de visitarlos.

Por ejemplo, si la organización posee oficinas repartidas por todo el país, pero la información de carácter personal se almacena de manera centralizada en la sede principal, ubicada en Barcelona, tiene sentido visitar esta sede principal, pero no visitar el resto. Aunque se puede seleccionar una muestra que esté en las proximidades de la sede principal para comprobar el nivel de concienciación del personal con relación a la protección de datos personales.

Sin embargo, si la organización almacena datos personales en ficheros de soporte papel y estos están ubicados en diferentes centros, aquí sí puede tener más sentido visitar estos centros, sobre todo para comprobar la seguridad física de acceso a las instalaciones, dado que esto también determina el nivel de protección de los datos personales.

El plan también debería incluir el detalle de las actividades que se llevarán a cabo, las personas que se entrevistarán (dirección, área de TI, área de RR. HH., etc.) e información de contacto del equipo auditor (teléfono, correo, etc.).

Es importante que nuestro Plan de Auditoría incluya una reunión de apertura, de unos 15 minutos el primer día, y una reunión de cierre, también de unos 15 minutos, el último día de auditoría. Además, cuando la auditoría se componga de varios días, se incluirá por cada día una reunión de *feedback*. En puntos posteriores explicaremos en qué consiste cada una de estas reuniones.

Adicionalmente al Plan de Auditoría, el equipo auditor puede desarrollar un programa de auditoría que establezca una programación de las auditorías que se propone realizar para los próximos años (cada año, cada dos años, etc.). Este programa puede tener más sentido cuando la organización tenga diferentes sedes y se requiera visitarlas todas en un plazo de tiempo.

Por ejemplo, en el programa se puede establecer que la mitad de las sedes se visiten el primer año y la segunda mitad, el siguiente año.

3) Revisión documental. Antes de comenzar la auditoría en las instalaciones de la organización es habitual solicitar la documentación que posea relativa a protección de datos. Esta documentación puede incluir acuerdos de confidencialidad con empleados, clientes y proveedores; políticas de seguridad; buenas prácticas de uso de activos; etc. Si la organización posee documentación relativa a la anterior LOPD, como por ejemplo, el documento de seguridad o algún informe de auditoría bienal, también puede ser revisado durante esta etapa.

La solicitud de esta documentación debe ser gestionada a través del auditor líder, que antes de nada firmará un acuerdo de confidencialidad con la organización y establecerá un canal seguro para la transferencia de información (por ejemplo, a través de ficheros cifrados, que pueden ser enviados por correo electrónico).

En esta etapa previa a la auditoría el equipo auditor ya puede empezar a detectar debilidades, que irá anotando en un documento de notas del auditor. En este documento, se debe incluir información sobre lo que se revisa y sobre las debilidades encontradas.

Como la auditoría se hace contra la LOPD-GDD, y esta se compone de artículos, siempre que detectemos una debilidad se deberá hacer referencia, de manera precisa, al artículo o punto de la normativa que se corresponda con la debilidad.

Estas debilidades que pueden ser identificadas durante el proceso de auditoría son conocidas también como «hallazgos» y, en caso de existir, deben transmitirse a la organización, al menos las que sean más críticas.

El principal objetivo de esta etapa es comprobar que la organización posee un mínimo de conocimiento y de información para cumplir con la LOPD-GDD. En algunos casos, se puede dar la situación de que, tras realizar la revisión de la documentación, determinemos que el cumplimiento de la organización con respecto a la LOPD-GDD sea muy débil y tengamos que decidir aplazar la auditoría para, de esta manera, darle tiempo a la organización a que se prepare mejor.

Por otra parte, un resultado satisfactorio de esta revisión documental no quiere decir que la organización ya cumpla al 100 % con la normativa porque el proceso de auditoría lo componen más etapas que se desarrollarán más adelante, por lo que es importante aclarar el objetivo de esta etapa previa con la organización.

1.1.2. Auditoría

El objetivo de la auditoría es comprobar que la organización cumple con la normativa de referencia.

Las actividades que componen la auditoría son las siguientes:

1) **Reunión de apertura.** Posterior a la revisión de la documentación, si todo ha ido bien, comenzaremos con la visita a las instalaciones de la organización. En esta visita, lo primero que realizaremos, de acuerdo al Plan de Auditoría, será una reunión de apertura en la que se darán a conocer los siguientes puntos:

- Objetivo de la auditoría de cumplimiento LOPD-GDD.
- Presentación del equipo auditor.
- Confirmación del Plan de Auditoría.
- Presentación de la compañía y de los interlocutores que participarán en la auditoría.
- Resolución de posibles dudas y aclaraciones.

Uno de los puntos más relevantes de esta primera toma de contacto con la organización es confirmar el Plan de Auditoría con las personas involucradas. Por tanto, el plan puede verse modificado en función de las peticiones que se puedan hacer durante esta reunión de apertura.

En esta primera reunión también es importante conocer al delegado de protección de datos en caso de que haya sido nombrado.

Otra cuestión importante que se debe aclarar durante esta primera reunión es conocer cómo actúa la organización con respecto a los datos personales que maneja: ¿actúa como responsable o como encargado de tratamiento?

Por otra parte, independientemente del proceso de auditoría en sí, esta primera reunión de apertura es imprescindible para conocer al personal de la organización. No debemos olvidar que la auditoría no se realizará contra personas, sino con ellas, para revisar el cumplimiento de una normativa. Esto básicamente quiere decir que el equipo auditor debe integrarse, en la medida de lo posible, con las personas de la organización para que estas puedan sentirse cómodas a la hora de facilitar la información que se requiera.

2) Trabajo de campo. Una vez confirmado el plan y establecido el primer contacto con el personal de la organización, es el momento del trabajo de campo. Este trabajo de campo puede incluir las siguientes tareas:

- **Revisión de documentos y registros:** si durante la etapa previa de revisión de documentos no dio tiempo de revisar toda la documentación o algunos documentos no se pudieron revisar por requisitos de confidencialidad definidos por la organización (la organización se puede negar a mandar documentos sensibles al exterior a pesar de utilizar canales seguros y estará en su derecho a no hacerlo), durante la auditoría será el momento de revisarlos. Por otra parte, los documentos que sí fueron revisados, serán comentados con la organización en el caso de que se haya detectado alguna debilidad o, si algún documento describía algún procedimiento concreto, durante la auditoría se revisará *in situ*. También se revisarán registros, que básicamente representan la evidencia de que se ha llevado a cabo un proceso. Por ejemplo, un procedimiento de auditoría puede ser un documento, mientras que el informe de auditoría, con las conclusiones, es un registro. Estos registros también se pueden revisar en la etapa previa de revisión documental, pero es más común revisarlos durante la auditoría.
- **Visitas a las instalaciones:** durante la visita a las instalaciones el equipo auditor debe observar cómo el personal de la organización desempeña su trabajo y sus correspondientes funciones para la protección de datos. Durante esta visita, cuando sea preciso, se podrán realizar preguntas al personal con el objetivo de conocer su nivel de implicación en la protección de datos. Algunas preguntas típicas pueden ser: ¿conoce cuáles son sus derechos con respecto a la protección de sus datos personales? o ¿cómo notificaría una brecha de seguridad relativa a una revelación de datos personales? A diferencia de las entrevistas definidas en el Plan de Auditoría, estas preguntas se harán a personal seleccionado de manera aleatoria, de manera que se pueda comprobar que el conjunto de empleados conoce los principios básicos de la LOPD-GDDD.
- **Entrevistas con personal:** las personas con las que hablemos en esta etapa habrán sido previamente seleccionadas y tendrán un perfil medio-alto en la jerarquía de la organización. Por ejemplo, podremos hablar con el responsable de gestionar las relaciones con proveedores para que nos muestre, si fuese posible, los acuerdos de confidencialidad firmados. Por otra parte, es importante crear un entorno agradable para que los audita-

dos se sientan cómodos a la hora de compartir información con nosotros. Cuanto más cómodos se sientan, más información proporcionarán.

Es importante incluir en nuestras notas de auditoría toda la información que vayamos recopilando, incluyendo el nombre y apellidos de las personas que participen en las entrevistas.

En cualquier caso, si detectamos alguna debilidad, no deberíamos asociarla nunca a una persona en concreto, es decir, no se deben personalizar los hallazgos. A efectos de la auditoría, no debemos olvidar que los incumplimientos son siempre de la organización, no de las personas que la componen.

Es decir, por ejemplo, si detectamos que un empleado está incumpliendo una política o no conoce cuáles son sus derechos con relación a sus datos personales, indicaremos lo siguiente:

«La organización no ha establecido los recursos necesarios para la concienciación en materia de protección de datos personales a todo el personal».

En lugar de: «Francisco José Navarro, por desconocimiento en la materia, no conoce la documentación relativa a la protección de datos que existe en la organización».

Por otra parte, es importante destacar que durante nuestras comprobaciones se pueden detectar incumplimientos no solo con respecto a la normativa, sino también con respecto a la documentación propia de la organización.

Por ejemplo, si detectamos que en un documento se establece que la organización manda información personal por correo electrónico y que esta siempre va cifrada, pero luego comprobamos que no se están cifrando estos correos, podemos identificarlo como un incumplimiento.

Para nuestras comprobaciones podremos realizar pruebas de cumplimiento, que nos ayudarán a determinar si la organización verdaderamente está cumpliendo o no con algún punto concreto de la normativa o de sus procedimientos.

Por ejemplo, en el caso que hemos visto antes del cifrado de la información personal en los correos, una prueba de cumplimiento podría consistir en solicitar a un empleado que nos muestre su buzón de salida del correo electrónico y buscar algún envío de datos personales. O seleccionar a un empleado de manera aleatoria y preguntarle qué haría para mandar un dato personal a través de correo electrónico.

3) Reuniones de *feedback*. A medida que se vayan detectando hallazgos durante el transcurso de la auditoría, deben ser transmitidos y explicados con claridad y con precisión a la organización. Además, como hemos visto en un punto anterior, quedarán también documentados en nuestras **notas de auditoría**.

Por otra parte, al final de cada jornada de auditoría, siempre que no sea la última jornada, se mantendrá una breve reunión con la organización y se le transmitirán las conclusiones, destacando los hallazgos detectados más relevantes.

El principal objetivo de estas reuniones es mantener informada a la organización de lo que se va detectado de forma que el último día, el de la **reunión de cierre**, no se encuentren con ninguna sorpresa de última hora.

Si no mantenemos estas reuniones de *feedback*, tampoco transmitimos los hallazgos que identificamos sobre la marcha a la organización y lo dejamos todo para el final, muy probablemente nos encontraremos con que la organización no los entiende o incluso no está conforme con nuestros hallazgos, lo cual significarán problemas de última hora para nosotros, que con la presión del último día, se podrá traducir en que tendremos que defender nuestro trabajo.

4) Reunión de cierre. Finalmente, una vez realizadas todas nuestras comprobaciones, podremos dar por concluida nuestra visita y, para ello, antes de abandonar las instalaciones de la organización, realizaremos una última reunión de cierre. En esta reunión, agradeceremos al personal involucrado su participación en el proceso de auditoría, y haremos un resumen de los hallazgos que hayamos detectado.

Si se han detectado incumplimientos relevantes, es importante transmitírselos en este momento a la organización, así como también informar de la obligación de tener que tratarlos y cerrarlos en un plazo tiempo definido, que habitualmente suele ser de tres meses.

Por otra parte, en esta última etapa no se suele entregar el informe final, pero se le informa a la organización que en los próximos días (habitualmente una semana), recibirá una versión borrador y, una vez confirmado este borrador, se hará entrega del informe final.

1.1.3. Posauditoría

El objetivo de la posauditoría es desarrollar el informe final de auditoría y tratar las desviaciones que se hayan detectado.

Las actividades que componen la posauditoría son las siguientes:

1) Desarrollo y envío del borrador del informe. Como se ha comentado en el punto anterior, en el plazo que se establezca con la organización, que habitualmente es de una semana, el equipo auditor se compromete a enviar una versión borrador del informe.

El contenido de este informe se detallará en el siguiente apartado, pero básicamente debe contener los hallazgos detectados, así como los puntos revisados y el estado de cumplimiento (cumple o no cumple). Además, el informe debe contener la dirección de los centros visitados, así como los nombres y apellidos de las personas entrevistadas.

Lo recomendable es entregar este borrador en formato no editable, es decir, es preferible usar .PDF a .DOC, para que de esta manera solo el equipo auditor pueda realizar los cambios que sean necesarios en el documento.

Como este informe puede contener información sensible de la organización, lo ideal es enviarlo a través de un canal seguro. Por ejemplo, se puede enviar por correo electrónico, pero en un fichero cifrado.

Una vez que lo reciba la organización, deberá revisarlo y transmitir al equipo auditor cualquier discrepancia, error o disconformidad que detecte y todo ello será analizado y consensuado entre ambas partes.

Para esta revisión del borrador del informe por parte de la organización, lo ideal es establecer un periodo, que puede ser de entre una y dos semanas, aunque este tiempo se puede acordar en función de las necesidades y la carga de trabajo de la organización.

2) Desarrollo y envío de informe final. Transcurrido el tiempo de la revisión del borrador del informe y consensuado el contenido del informe, se completará la versión final y se enviará a la organización. Para este envío se deberá establecer un canal seguro.

Con respecto al formato de este informe final, nuevamente lo deseable es enviarlo en formato no editable, es decir, en .PDF.

3) Elaboración del Plan de Acciones Correctivas. Si durante la auditoría se han detectado incumplimientos o hallazgos que se pueden convertir en incumplimientos, la organización tendrá que desarrollar un **Plan de Acciones Correctivas**.

Este Plan de Acciones Correctivas tiene como principal objetivo llevar a cabo un tratamiento de estos incumplimientos o hallazgos para poder corregirlos.

Para este tratamiento, por cada incumplimiento la organización deberá completar la siguiente información:

a) Análisis de la causa raíz: es necesario determinar el origen del incumplimiento.

Por ejemplo, si el incumplimiento detectado es que los empleados no están concienciados en material de protección de datos personales, el origen puede ser la falta de presupuesto.

b) Corrección: es necesario determinar qué va a hacer la organización para corregir, a corto plazo, el incumplimiento detectado.

Siguiendo el ejemplo del punto anterior, la organización podría establecer contratar a una persona externa, experta en la LOPD-GDD, para que dé charlas de concienciación a todo el personal de la organización.

c) Acción correctiva: es necesario determinar qué va a hacer la organización para que el incumplimiento no se vuelva a repetir en el futuro.

Siguiendo con el ejemplo de puntos anteriores, la organización podría establecer que anualmente es necesario establecer una partida presupuestaria específica para el cumplimiento de la LOPD-GDD y esto incluye todo lo relativo a la concienciación del personal.

Además, para cada incumplimiento, la organización deberá proporcionar información sobre la persona encargada de llevar a cabo el tratamiento, así como un plazo límite para cerrar el tratamiento.

Junto con toda esta información, si en el momento del envío del Plan de Acciones Correctivas, la organización ha realizado ya alguna acción de tratamiento, deberá enviar también evidencias al equipo auditor. Por ejemplo, si ya ha seleccionado y contratado a un experto, para concienciar al personal, puede mandar el acuerdo firmado con esta persona, donde se especifique el servicio que va a ofrecer.

Si la organización no ha desarrollado nunca un Plan de Acciones Correctivas, es importante informarle al respecto. Por ejemplo, durante la reunión de cierre, siempre que obviamente se hayan detectado incumplimientos y la organización tenga la obligación de enviar el Plan de Acciones Correctivas. En el siguiente apartado se dará mayor información sobre cómo tratar las acciones correctivas.

4) Aprobación del Plan de Acciones Correctivas. Cuando la organización complete y envíe el Plan de Acciones Correctivas al equipo auditor, este procederá a su revisión.

Durante esta revisión, el equipo auditor comprobará que la información proporcionada es correcta y podrá solicitar mayor información cuando lo considere necesario.

Por ejemplo, si la organización indica que ha contratado a un experto externo, pero no lo evidencia con ningún registro, el equipo auditor deberá solicitarlo.

Una vez comprobada toda la información y todos los registros, el equipo auditor deberá proporcionar su conformidad y dará por aprobado el Plan de Acciones Correctivas.

En este punto es importante destacar que en el Plan de Acciones Correctivas se pueden establecer fechas de cierre, de modo que a la hora de presentar el Plan de Acciones Correctivas, las acciones incluidas no tienen por qué estar cerradas (aunque sí que estarán planificadas).

Para aquellas acciones pendientes, el equipo auditor deberá realizar un seguimiento para comprobar que efectivamente se traten los incumplimientos o hallazgos y se cierre el Plan de Acciones Correctivas de acuerdo a lo establecido por la propia organización.

5) Seguimiento del Plan de Acciones Correctivas. Como se ha comentado en el punto anterior, el equipo auditor debería realizar un seguimiento del Plan de Acciones Correctivas si este contiene acciones que han quedado abiertas en el tiempo.

Este seguimiento puede ser en remoto, es decir, no es necesario volver a visitar las instalaciones de la organización para comprobar que se han corregido los incumplimientos, aunque si se considera necesario, se pueden mantener conversaciones telefónicas o videollamadas con el personal afectado para que de esta manera pueda demostrar el tratamiento realizado.

1.2. Elaboración del informe de auditoría: aspectos básicos e importancia del informe de auditoría

Como se ha visto en el subapartado anterior, el informe de auditoría contempla los resultados de nuestras comprobaciones, por lo que es un elemento muy importante, dado que sin él la organización no tiene información precisa sobre lo que tiene que corregir para cumplir o adecuarse a la normativa.

Pensad también que el informe pretende mostrar la situación de la organización en el momento de la realización de la auditoría y esto es muy útil para futuras auditorías porque permite al equipo conocer cómo ha evolucionado la organización con el transcurso del tiempo.

Por otra parte, el equipo auditor suele, y debe, transmitir a la organización mucha información sobre lo que va detectando sobre la marcha. Esta información que transmite el equipo auditor está basada en su experiencia y en su conocimiento sobre la LOPD-GDD, que suele ser muy enriquecedor, entre otras cosas porque el equipo auditor aporta una visión objetiva con la ventaja de haber auditado otras empresas del mismo sector u otro distinto.

Pero si toda esta información no se registra o no se documenta en ningún lugar, lo habitual es que se olvide y se pierda. Por tanto, el informe de auditoría es también una forma de que la organización recuerde todas las cuestiones que surgieron y trataron durante la auditoría.

Sabiendo lo importante que es el informe de auditoría, la pregunta que nos queda por hacer es: ¿qué información exactamente tiene que contener? La respuesta a esta pregunta nos la proporciona la guía que comentamos en el apartado anterior: la **ISO 19011**.

De acuerdo a la versión 2018 de esta guía, es decir, de acuerdo a la ISO 19011:2018, el informe de auditoría debe de contener la siguiente información:

1) Objetivos de auditoría: por ejemplo, comprobar el cumplimiento de la organización con respecto a la LOPD-GDD.

2) Alcance de la auditoría: generalmente el alcance de la auditoría de cumplimiento de la LOPD-GDD contempla toda la organización, salvo que se requiera una auditoría parcial sobre un área, departamento o ubicación concretos.

3) Identificación del cliente: se suelen incluir datos de contacto de la organización, como el email, teléfono, etc. La persona de contacto puede ser, por ejemplo, el delegado de protección de datos de la organización, el gerente o el responsable del área que gestiona la protección de datos personales.

4) Identificación del equipo auditor: se suelen incluir datos de contacto del equipo auditor, como el email, teléfono, etc. En este caso, si el equipo auditor está formado por varias personas, habitualmente se proporcionan los datos del auditor líder.

5) Fechas, horarios y localizaciones donde se realizaron las actividades de auditoría: se suele incluir información detallada de los días en los que se ha realizado la auditoría, como los horarios y las sedes que se hayan visitado. Generalmente esta información se corresponderá con el Plan de Auditoría, salvo que se haya tenido que modificar sobre la marcha, en cuyo caso se actualizará en el informe.

6) Criterios de auditoría: en este punto debemos indicar en qué referencia nos basamos para realizar la auditoría, que en nuestro caso está claro, la referencia es la LOPD-GDD. Además, también nos basaremos en los procedimientos, procesos y documentos de la organización, dado que, durante la auditoría, además de revisar el cumplimiento de la LOPD-GDD también revisaremos el cumplimiento de la organización con sus propios procedimientos, procesos y documentos.

7) Hallazgos de auditoría y evidencias relacionadas: en este punto se incluirán todos los hallazgos que se detecten durante la auditoría. Generalmente existen diferentes tipos de hallazgos que se describirán más adelante. Por cada hallazgo, es importante incluir el punto o artículo de la LOPD-GDD con el

que esté relacionado el hallazgo y las evidencias que se hayan detectado. Por ejemplo, se pueden incluir capturas de pantalla del contenido de documentos, fotografías del entorno observado, etc. También es importante establecer un criterio a la hora de ordenar y representar los hallazgos en el informe.

Por ejemplo, un criterio puede ser incluir primero los hallazgos menos importantes y luego los que pueden representar, o representan, un incumplimiento con respecto a la normativa. Otro criterio puede ser el contrario, es decir, incluir primero los hallazgos que representan un incumplimiento con respecto a la normativa y después los hallazgos que son menos relevantes.

8) Conclusiones de auditoría: es recomendable que este apartado no sea demasiado extenso (máximo de una página) y básicamente debe contener las apreciaciones globales del equipo auditor, destacando los hallazgos más relevantes e indicando resumidamente en qué medida la organización cumple o no con la normativa. Por otra parte, cuando se hayan identificado incumplimientos y sea preciso el envío de un plan de acciones correctivas, se indicará también en este apartado de conclusiones, indicando el tiempo que la organización tiene para presentarlo.

Es importante dejar claro en el informe que la auditoría generalmente se realiza sobre una muestra de la organización, es decir, si existen cincuenta empleados, muy probablemente no podremos entrevistarlos a todos, en su lugar, seleccionaremos una muestra. Puede ocurrir lo mismo con la documentación: si la organización posee diez acuerdos de confidencialidad con proveedores de servicio, podremos seleccionar dos o tres para revisar su contenido.

También es importante indicar en el informe cualquier incidencia que se haya podido producir entre el equipo auditor y la organización.

Por ejemplo, si el equipo auditor identifica un incumplimiento y la organización no está conforme, se indicará en el informe. También puede ocurrir que el equipo auditor solicite revisar un documento, pero la organización no lo permita por motivos de confidencialidad, en cuyo caso, también se indicará en el informe.

Por otra parte, en el caso de que no se haya podido cumplir con el calendario definido en el plan, visitar algún centro, revisar algún proceso o entrevistar a alguna persona de las que se identificaron en el Plan de Auditoría, igualmente se añadirá en el informe, incluyendo información sobre las razones que han impedido realizar estas actividades.

Cuando sea necesaria una visita adicional, posterior a la auditoría, para comprobar la adecuada corrección de un incumplimiento detectado, se puede incluir en el informe la fecha de esta próxima visita.

Generalmente, los informes de auditoría se generan después de realizar la visita a las instalaciones de la organización¹ porque así se dispone de más tiempo para su elaboración y de esta manera también se puede consensuar su contenido con la organización. Pero en algunos casos, cuando la organización sea pequeña y la auditoría no haya sido compleja, se puede considerar desarrollar

⁽¹⁾ Como vimos en un apartado anterior, el plazo suele ser de una semana, empezando a contar después de concluir la auditoría.

el informe completo durante la auditoría y presentar la versión final el último día de auditoría. En cualquier caso, si el informe contiene incumplimientos, la organización igualmente tendrá que presentar el correspondiente Plan de Acciones Correctivas, tal y como se detalló en apartados anteriores.

Por último, dada la sensibilidad de la información que puede contener el informe, este se suele clasificar como «confidencial» y así deberemos indicarlo, por ejemplo, incluyendo algún apartado específico dentro del informe, estableciendo de manera explícita que toda la información contenida en el mismo es confidencial.

1.3. Ejecución y seguimiento de acciones correctoras

Como ya hemos visto en el subapartado anterior, durante la auditoría se pueden detectar hallazgos y pueden existir de diferentes tipos (figura 2), los cuales se muestran a continuación:

1) No conformidad mayor: representa un incumplimiento grave con respecto a la normativa, por ejemplo, porque no se cumple un requisito completo de la LOPD-GDD.

Si la organización ha recopilado datos de carácter personal sin el consentimiento explícito de los interesados, claramente se puede identificar como una no conformidad mayor (el artículo 6 de la LOPD-GDD habla del «Tratamiento basado en el consentimiento del afectado»).

2) No conformidad menor: representa un incumplimiento concreto contra un punto específico de un artículo de la normativa, es decir, no se incumple un requisito completo, pero sí una parte.

Por ejemplo, si se establece el deber de confidencialidad a todo el personal implicado en el tratamiento de datos personales, pero esta obligación no se mantiene después de finalizar la relación contractual con la organización, se puede identificar como una no conformidad menor, dado que se incumpliría el punto 3 del artículo 5 de la LOPD-GDD («Deber de confidencialidad»).

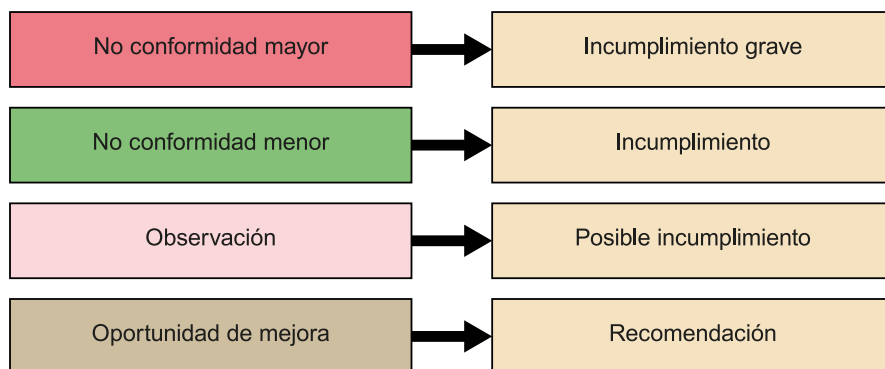
3) Observación: realmente no representa un incumplimiento, pero requiere que la organización lleve a cabo un tratamiento. En caso de que la organización no lleve a cabo este tratamiento en el futuro, en una auditoría posterior se puede convertir en no conformidad.

Si se detecta que la organización ha nombrado de manera informal un delegado de protección e incluso se encuentran registros de este nombramiento, pero no ha sido aprobado aún por la alta dirección de la organización, se puede identificar como observación. En el capítulo III de la LOPD-GDD, se encuentran los artículos «34. Designación de un delegado de protección de datos», «35. Cualificación del delegado de protección de datos», «36. Posición del delegado de protección de datos» y «37. Intervención del delegado de protección de datos en caso de reclamación».

4) Oportunidad de mejora: únicamente representa una recomendación desde el punto de vista, y experiencia del equipo auditor, por lo que en este caso la organización no tiene la obligación de llevar a cabo un tratamiento (ni en el presente, ni en el futuro). No obstante, es importante transmitir a la organización que, aun no siendo obligatorio el tratamiento, le puede ayudar a mejorar.

Por ejemplo, se puede identificar una oportunidad de mejora si la organización está utilizando un algoritmo para cifrar datos sensibles y puede utilizar otro más fuerte (AES 256, en lugar de AES 128).

Figura 2. Hallazgos del proceso de auditoría



Además, durante la auditoría también se pueden identificar **puntos fuertes**. Estos representan una actividad, proceso o cualquier otro elemento que la organización está realizando muy bien. En este punto, el criterio que se puede seguir para identificar un punto fuerte es comparar la organización con otras que el equipo auditor haya auditado en el pasado. Si la efectividad del funcionamiento de un elemento de la organización es superior al de otras empresas, se puede identificar como punto fuerte.

Por ejemplo, si la organización está invirtiendo una gran parte de su presupuesto anual en concienciar a todo su personal en la protección de datos personales, con cursos, charlas y webinars, y además realiza auditorías para comprobar el cumplimiento, se podría identificar como punto fuerte.

Siempre es importante identificar algún punto fuerte (cuando sea posible) porque de esta manera la organización puede sentir que en el proceso de auditoría no todo es malo.

Todos estos conceptos son importantes no solo para el auditor, sino también para el auditado, por lo que si la organización no conoce la terminología, es deber del equipo auditor aclararla.

En cuanto a las **acciones correctivas**, siempre son necesarias para el tratamiento de todas las debilidades identificadas durante la auditoría, aunque habitualmente solo se registran las acciones correctivas derivadas de las no conformidades (mayores y menores), es decir, no se suelen registrar las acciones correctivas derivadas de las observaciones y oportunidades de mejora.

Sin embargo, registrar las acciones correctivas de las observaciones y oportunidades de mejora tiene un importante beneficio, ya que permite hacer un seguimiento de lo que se ha hecho y de lo que queda por hacer. Esto es especialmente importante en el caso de las observaciones porque, como ya se ha comentado en un punto anterior, si no se tratan, se pueden convertir en no conformidad.

Por otra parte, como vimos en un punto anterior, cada acción correctiva debe recopilar, al menos, la siguiente información:

- Análisis de la causa raíz (origen)
- Corrección (solución inmediata)
- Acción correctiva (solución completa)
- Responsable
- Plazo

Es responsabilidad del equipo auditor comprobar que la información registrada por la organización para cada desviación es correcta. No obstante, para evitar problemas, es recomendable que el equipo auditor, antes de finalizar la auditoría, aclare los conceptos e incluso, si es posible, proporcione algún ejemplo.

Veamos a continuación cómo debería actuar el equipo auditor ante la siguiente no conformidad mayor.

Ejemplo de actuación ante una no conformidad mayor

La organización realiza un tratamiento de datos personales, pero no está basado en el consentimiento de los afectados (incumplimiento del artículo 6).

Una acción correctiva incorrecta sería la siguiente:

- **Análisis de la causa raíz:** Por falta de presupuesto la organización no ha contado con los recursos adecuados para cumplir con todos los requisitos definidos por la LOPD-GDD. Esto incluye la solicitud del consentimiento previo al tratamiento de los datos.
- **Corrección:** Se manda un comunicado a todos los afectados indicando lo ocurrido y solicitando el consentimiento expreso para el tratamiento de sus datos personales.
- **Acción correctiva:** Se acuerda una partida presupuestaria específica para contar con apoyo externo especializado en la LOPD-GDD que les asesorará en todas las cuestiones relativas a esta normativa.
- **Responsable:** Gerente TI.
- **Plazo:** 31 de diciembre.

Y ahora veamos la versión correcta:

- **Análisis de la causa raíz:** Previo al tratamiento de datos personales, la organización no solicita el consentimiento a los interesados.
- **Corrección:** Se solicita consentimiento.
- **Acción correctiva:** Cada vez que entre un nuevo empleado, se le solicitará el consentimiento antes de tratar sus datos personales.
- **Responsable:** Gerente TI.
- **Plazo:** 31 de diciembre.

Por otra parte, siempre es responsabilidad única y exclusiva de la organización definir las acciones correctivas y ejecutar las actividades que sean precisas. Es decir, en ningún caso el equipo auditor puede formar parte del proceso de tratamiento de una acción correctiva.

2. Auditoría de sistemas de información

Hoy en día, los datos personales se pueden encontrar principalmente en dos formatos: **papel** y **electrónico**. En la anterior LOPD, los datos en formato electrónico se conocían como «ficheros automatizados», mientras que los que se encontraban en formato papel se conocían como «ficheros no automatizados». Además, existía un tercer tipo de formato, los «archivos mixtos», cuando los datos se encontraban en ambos formatos, es decir, en papel y en electrónico.

En cualquier caso, la tendencia es, cada vez más, digitalizar toda la información, incluyendo los datos personales, por lo que estos datos terminan almacenándose en sistemas de información.

Según el estándar ISO/IEC 27000, el cual contiene un apartado de vocabulario con términos específicos de seguridad de la información, un **sistema de información** se define de la siguiente manera:

«A set of applications, services, information technology assets, or other information-handling components».

Por tanto, los servidores, estaciones de trabajo, aplicaciones, medios de almacenamiento, etc. que utilizemos para el manejo de información podemos considerarlos como sistemas de información.

Estos sistemas de información pueden tener riesgos asociados, que será necesario identificar y tratar. Es decir, es necesario gestionar los riesgos asociados a los sistemas de información para, de esta manera, poder proteger los datos de cualquier naturaleza, incluyendo los datos personales.

Dentro de la gestión de estos riesgos, forman parte también las **auditorías de sistemas de información**, que se detallarán en el siguiente subapartado.

2.1. La función de la auditoría en los sistemas de información. Conceptos básicos. Estándares y directrices de auditoría de seguridad de la información

Si hablamos de estándares internacionales relacionados con los sistemas de información, el más popular y conocido mundialmente es sin duda ISO/IEC 27001.

El estándar ISO/IEC 27001 define una serie de requisitos para el establecimiento de un **sistema de gestión de seguridad de la información** (SGSI), es decir, tiene como principal objetivo la protección de la información y, para ello, se basa en un modelo de mejora continua, que tiene como núcleo principal la gestión de riesgos (riesgos relativos a la seguridad de la información).

En la práctica, lo anterior quiere decir que la información está en sistemas de información y nos apoyamos en un estándar internacional para gestionar su seguridad, es decir, para proteger la información.

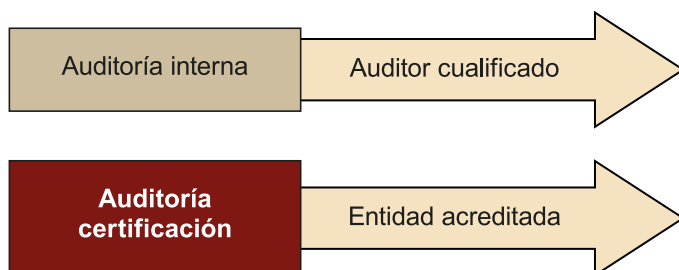
Por tanto, si implementamos este sistema en una organización, es decir, si implementamos un SGSI en una empresa para gestionar la seguridad, entre otras cosas, tendremos que identificar riesgos y tratarlos.

Una vez gestionados estos riesgos e implementado el SGSI, será necesario realizar una auditoría interna, que puede seguir el mismo proceso que se estableció en el punto anterior cuando se habló de las auditorías de cumplimiento LOPD-GDD.

Además, posterior a la auditoría interna, también se puede llevar a cabo una auditoría de certificación, que será llevada a cabo por un organismo o entidad de certificación.

La diferencia principal entre la auditoría interna y la auditoría de certificación, como se puede observar en la figura 3, es que las entidades de certificación suelen estar acreditadas por el organismo nacional acreditador de cada país (en el caso de España, el organismo acreditador es ENAC), lo cual proporciona garantías de **objetividad, imparcialidad y profesionalidad**. Una vez concluida la auditoría, si la organización ha superado el proceso, la entidad certificadora podrá emitir un certificado ISO/IEC 27001, que estará acreditado por ENAC.

Figura 3. Tipos de auditoría SGSI



Las auditorías internas, en cambio, puede realizarlas cualquier profesional con experiencia en seguridad de la información, siendo el único requisito que no hayan participado en el proceso de implementación del SGSI. Por tanto, en este caso el auditor no puede emitir un certificado ISO/IEC 27001 acreditado por otra entidad.

En cualquier caso, la realización de la auditoría interna es un requisito en la ISO/IEC 27001 (y en todos los sistemas de gestión como ISO 9001, ISO 20000, ISO 14001, etc.), y puede ayudar a identificar desviaciones, antes de la auditoría de certificación.

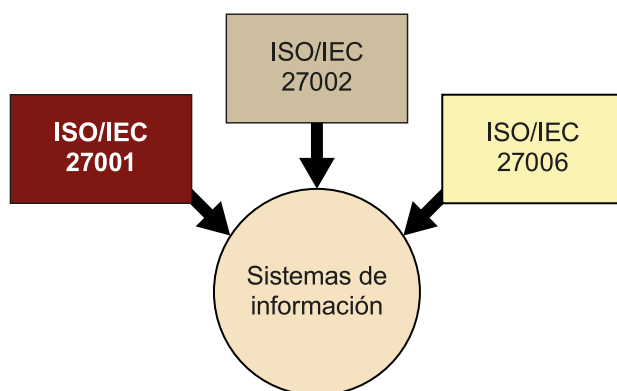
Por otra parte, las entidades certificadoras, para poder acreditarse, tienen que cumplir con otro estándar, el ISO/IEC 27006. Es decir, cualquier entidad certificadora que quiera estar acreditada en España por ENAC tiene que implementar y cumplir con la ISO/IEC 27006.

La ISO/IEC 27001 dispone de un anexo A, que incluye ciento catorce controles de seguridad de la información, que provienen de otro estándar: ISO/IEC 27002.

La principal diferencia entre la información que aparece en el anexo A de la ISO/IEC 27001 y el contenido de la ISO/IEC 27002 es que en el anexo A aparece solo una breve descripción de cada control, mientras que en la ISO/IEC 27002 se puede encontrar una guía detallada para saber cómo implementar cada control.

Por tanto, la base para auditar y certificar nuestros sistemas de información la componen los tres estándares que muestra la figura 4.

Figura 4. Estándares ISO



Adicionalmente, las entidades certificadoras pueden desarrollar sus propios esquemas de certificación (que también podrían acreditar). Es decir, por ejemplo, una entidad certificadora puede desarrollar su propio esquema basado en el RGPD, acreditarlo y certificarlo.

No obstante, en la práctica existen muchas organizaciones que cuando quieren contratar un servicio a un proveedor externo lo primero que hacen es una auditoría a los sistemas de información de este proveedor para comprobar la seguridad de sus sistemas. Para llevar a cabo esta auditoría se basan principalmente en los controles del anexo A de la ISO/IEC 27001, dado que son medidas concretas que la organización establece para la protección de la información.

Como se comentó anteriormente, el núcleo de la ISO/IEC 27001 es la gestión de riesgos, para la cual es necesario analizar riesgos y luego tratarlos.

Para el tratamiento necesitaremos controles de seguridad y es aquí donde entra en escena el anexo A, dado que nos ayudará a seleccionar los controles que necesitemos para el tratamiento de los riesgos que hayamos identificado durante el análisis.

Este anexo A nos puede ayudar como guía durante nuestra auditoría a los sistemas de información para conocer los controles de seguridad que existen, o no, en la organización y que podrían suponer un riesgo de seguridad de la información.

Por otra parte, también es muy habitual que durante la revisión de los controles se determine el **nivel de madurez** en aquellos casos donde obviamente exista el control. Este nivel de madurez se determina basándose en los criterios del **modelo CMMI** que están desarrollados en la figura 5.

Figura 5. Niveles de madurez según el modelo CMMI

0 - Incompleto	No existe control o está documentado en la teoría, pero no se ejecuta en la práctica.
1 - Realizado	Existe control y funciona, pero no de forma precisa y no está documentado ni formalizado en la empresa.
2 - Gestionado	Control definido, documentado, planificado y actualizado, pero no se ha ejecutado.
3 - Establecido	Control implementado que funciona, se mantiene, se actualiza y se lleva a cabo de acuerdo a un plan.
4 - Predecible	Nivel 3 + KPI
5 - Optimizado	Nivel 4 + Mejora continua, optimización de procesos, herramientas, etc.

Lectura recomendada

La lista completa de los controles puede consultarse en el anexo A de la ISO/IEC 27001 o bien también en la ISO/IEC 27002, por lo que se recomienda su atenta lectura.

Enlace a la página oficial de ISO/IEC 27001:
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>

Enlace a la página oficial de ISO/IEC 27002:
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>

Además, la organización también puede llevar a cabo auditorías técnicas sobre los sistemas de información, es decir, se pueden llevar a cabo análisis de vulnerabilidades y pruebas de intrusión.

Para este tipo de auditorías técnicas, podemos contemplar tres escenarios diferentes:

- **Pruebas de caja negra:** cuando no tenemos información técnica de la organización.
- **Pruebas de caja blanca:** cuando poseemos información técnica proporcionada por la organización.
- **Pruebas de caja gris:** cuando poseemos parte de información técnica proporcionada por la organización, pero no tenemos toda la información.

También es importante saber diferenciar entre un simple **análisis de vulnerabilidades** que nos permitirá conocer cuáles son las posibles vulnerabilidades técnicas que afectan a los sistemas de información, y unas **pruebas de intrusión**, con las que aprovecharemos las vulnerabilidades para poder acceder a los sistemas y, de esta manera, comprometer la seguridad de los sistemas vulnerados.

No obstante, en estas pruebas también se debe considerar el componente humano, es decir, muchos ataques se producen porque una persona ha abierto un fichero, un correo o simplemente ha proporcionado unas claves de acceso a una persona que la ha llamado por teléfono.

Los ataques que tienen como foco principal las personas y como objetivo capturar información sensible, se conocen como **ataques de ingeniería social**, y es muy recomendable contemplarlos en nuestras auditorías de sistemas de información.

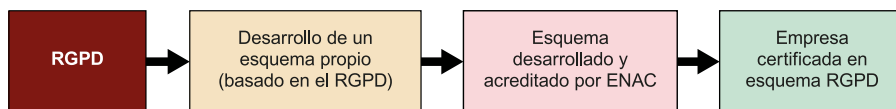
2.2. Control interno y mejora continua. Buenas prácticas.

Integración de la auditoría de protección de datos en la auditoría de seguridad de la información

Como se ha comentado en el subapartado anterior, las entidades certificadoras pueden desarrollar esquemas propios de certificación y, una vez acreditados, pueden emitir certificados de estos esquemas. En resumen, como muestra la figura 6, una entidad certificadora puede desarrollar su propio esquema basándose, por ejemplo, en los principios del RGPD o de la LOPD-GDD. Una vez desarrollado el esquema, puede solicitar su acreditación a ENAC (en el caso específico de España), y tras conseguir la acreditación, la cual se otorgará si la entidad certificadora cumple con ciertos requisitos, puede emitir certificados a

las empresas que soliciten una auditoría de certificación RGPD. Por supuesto, el certificado se emitirá a la empresa que lo solicite, solo si cumple con los requisitos definidos por el esquema desarrollado por la entidad certificadora.

Figura 6. Estados por los que puede pasar un esquema de certificación



Por lo tanto, una entidad certificadora puede desarrollar un esquema de certificación RGPD y la empresa que cumpla con sus requisitos, tras una evaluación por parte de la entidad certificadora, podría obtener su certificación.

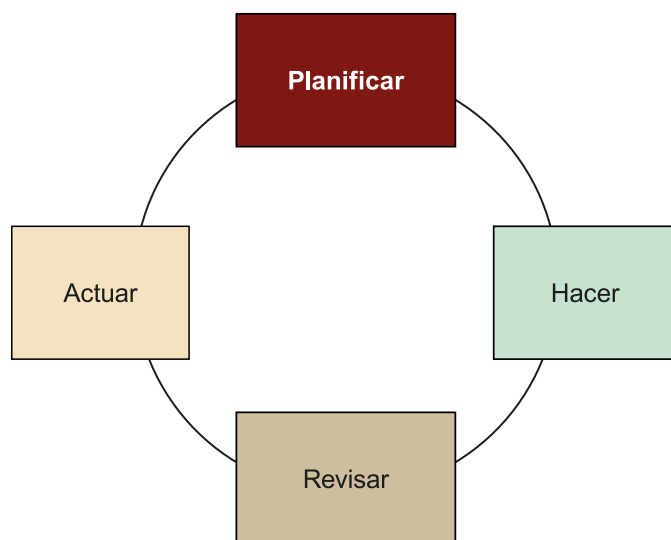
No obstante, los esquemas de certificación habituales, como ISO 27001, ISO 9001, etc., suelen estar basados en modelos de mejora continua, por lo que, generalmente, las entidades certificadoras, para no complicarse la vida, cuando desarrollan su esquema RGP, también le añaden el modelo de mejora continua.

Una razón para añadir este modelo, que no establece el RGPD o la LOPD-GDD, es que permite definir actividades que se tienen que repetir continuamente y que nos van a ayudar a mejorar.

Los modelos de mejora continua, además, son muy conocidos en todo el mundo y están muy presentes en empresas de todos los sectores, sobre todo en aquellas donde existe un sistema de gestión basado en un estándar ISO, porque estos sistemas se apoyan también en la mejora continua.

Uno de los modelos de mejora continua más conocidos es el **ciclo de Deming**, o ciclo PDCA, que muestra la figura 7 y está compuesto por cuatro etapas: planificar (*plan*), hacer (*do*), revisar (*check*), y actuar (*act*).

Figura 7. Modelo PDCA



Si seguimos este modelo, en la primera etapa (planificar) tenemos que planificar las actividades que queremos implementar. En la siguiente etapa (hacer), hay que ejecutar las actividades planificadas. A continuación (revisar), se revisan si las actividades se han ejecutado de acuerdo a como las planificamos. Finalmente, en la última etapa (actuar), es necesario corregir todas aquellas actividades que no se estén realizando de acuerdo a como lo planificamos.

Ejemplo de aplicación del ciclo de Deming

Por ejemplo, podemos imaginar que queremos comprarnos un ordenador nuevo. En este caso, lo primero que hacemos, generalmente, es **planificar** qué ordenador queremos comprar basándonos en la marca, modelo, capacidad de disco duro, memoria RAM, CPU, etc., pero también teniendo en cuenta cuánto nos podemos gastar, cómo lo podremos pagar, dónde, etc.

Una vez elegido el ordenador, el presupuesto que nos podemos gastar y cómo lo queremos pagar, buscamos tiendas por internet hasta que encontramos la opción que mejor se ajusta a nuestros requisitos y nos disponemos a **hacer** la compra del ordenador.

Cuando lo recibimos en casa, lo primero que hacemos siempre es **revisar** que lo que hemos comprado se corresponde con lo que hemos pedido por internet. Así que, entre otras cosas, verificamos la capacidad del disco duro, memoria, etc.

Si comprobamos que, por ejemplo, en la compra indicamos que queríamos un portátil de quince pulgadas y nos han enviado un portátil de trece pulgadas, tenemos que **actuar** y reclamar a la tienda para que nos entreguen lo que compramos o para que nos devuelvan el dinero.

Este mismo ejemplo se puede utilizar en otros ámbitos como en el del RGPD:

- Se planifica cómo abordar los diferentes requisitos establecidos por el RGPD o la LOPD-GDD. Esto implicará la definición de actividades, desarrollo de documentos, políticas, etc. En otras palabras, se desarrolla un Plan de Proyecto de Adecuación al RGPD.

- Se implementan todas las actividades definidas en el punto anterior, cosa que incluye ejecutar y completar el Plan de Proyecto de Adecuación al RGPD.
- Se revisa si el proyecto se ha implementado de acuerdo a lo que se estableció en el plan. Para hacerlo, se comprueba si se han desarrollado todos los productos definidos en el Plan de Proyecto, es decir, se comprueba si la organización cumple con todos los requisitos del RGPD.
- Por último, en el caso de que falle algo, se corrige. Si algún requisito no se cumple, habrá que implementar las acciones que sean necesarias para cumplirlo.

Por tanto, si a la base del RGPD le añadimos un modelo de mejora continua, basado, por ejemplo, en el PDCA, podremos planificar las acciones que sean necesarias para cumplir con esta ley, implementarlas, revisarlas y actuar en caso de que sea necesario.

Esto al final se traduce en que muchas empresas tendrán su modelo de mejora continua con el que se apoyarán para gestionar el cumplimiento con el RGPD o la LOPD-GDD.

Asimismo, los modelos de mejora continua son el núcleo de los sistemas de gestión, que pueden estar basados en diferentes estándares ISO dependiendo del propósito:

- Seguridad de la información: ISO
- Servicios TI: ISO 20000
- Continuidad del negocio: ISO
- Calidad: ISO 9001
- Medio ambiente: ISO 14001

Nota

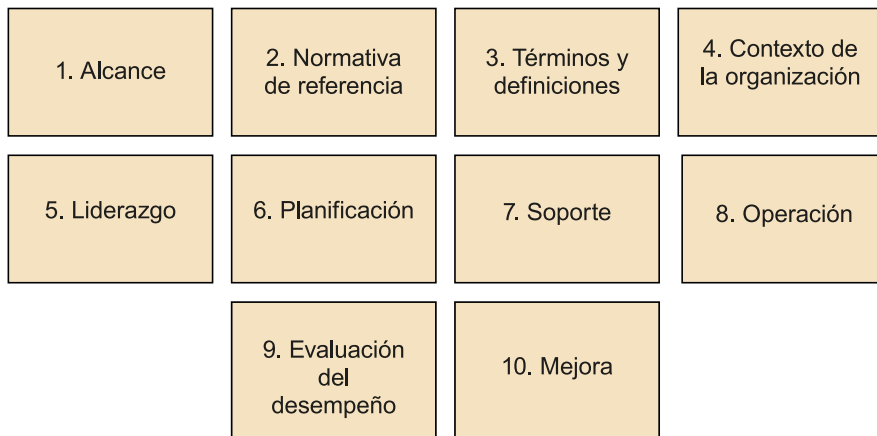
Existen muchos más sistemas de gestión y estándares ISO, pero aquí solo se dan a conocer lo más conocidos.

Todos los estándares ISO poseen puntos en común, lo que significa que, si una organización tiene implementados varios sistemas de gestión, podría integrarlos y tener un único sistema de gestión integrado. En el caso de que no estén integrados, la buena práctica será siempre recomendar a la organización que los integre, dado que se puede evitar repetir trabajo y tener un sistema más eficiente.

Es muy probable que un auditor, cuando realice auditorías de protección de datos, encuentre sistemas de gestión en las empresas que visita, por lo que es importante que tenga unos conocimientos mínimos de estos sistemas de gestión. Cuanto más conocimiento tenga el auditor, más podrá aportar a la organización y esta estará más satisfecha con la auditoría.

Actualmente los estándares ISO más populares (ISO 27001, ISO 9001, ISO 14001, ISO 22301 e ISO 20000) poseen un esquema común, compuesto principalmente por diez puntos, referenciados en la figura 8.

Figura 8. Estructura común de sistemas de gestión de los estándares ISO



Está claro que cada estándar define sus requisitos propios, pero es importante saber que la estructura es la misma, para así facilitar la integración, que suele ser lo recomendable.

En definitiva, si tenemos que realizar una auditoría en una empresa que tiene un sistema de gestión de seguridad de la información basado en ISO/IEC 27001 y además tiene la LOPD-GDD, podremos usar como guía la estructura de la ISO/IEC 27001 (los diez apartados comunes entre los sistemas de gestión) e ir comprobando si la organización cumple con los requisitos de cada esquema (ISO/IEC 27001 y LOPD-GDD).

Enlace de interés

La Agencia Española de Protección de Datos dispone en su página web de un listado de cumplimiento normativo que podréis utilizar en vuestras auditorías.

Al mismo tiempo, podemos contar con la ISO/IEC 27701, que es una extensión de la ISO/IEC 27001 e ISO/IEC 27002, pero enfocada principalmente a la protección de datos personales.

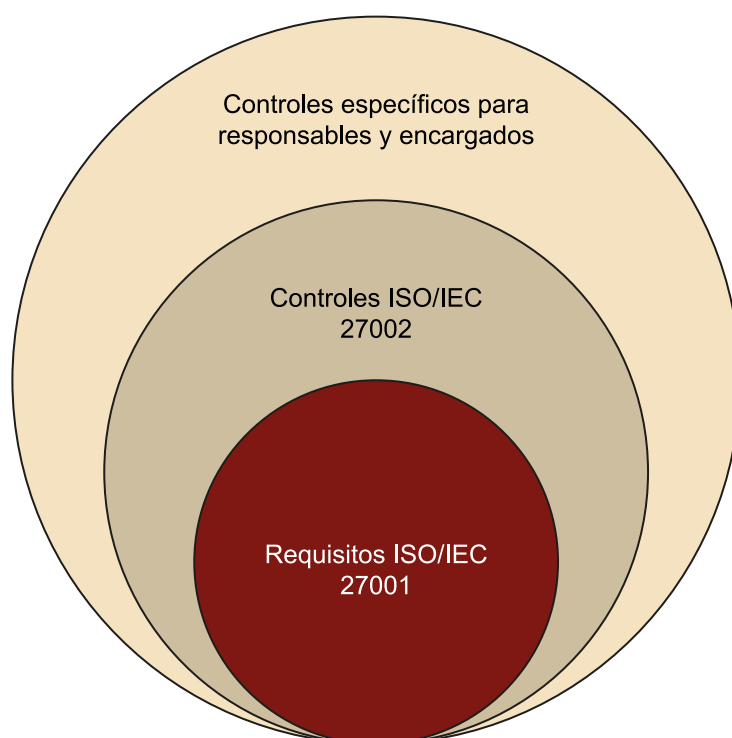
Este estándar define los mismos requisitos que la ISO/IEC 27001, pero añadiendo algunos más específicos relativos a la privacidad (de datos personales). Así pues, define un sistema de gestión de la información de privacidad (SGIP).

Por otra parte, utiliza los mismos controles de la ISO/IEC 27002, pero añadiendo información en la guía de implementación de algunos de ellos, con el enfoque de la privacidad.

Y además, establece controles específicos orientados tanto a los responsables como a los encargados de la información de identificación personal.

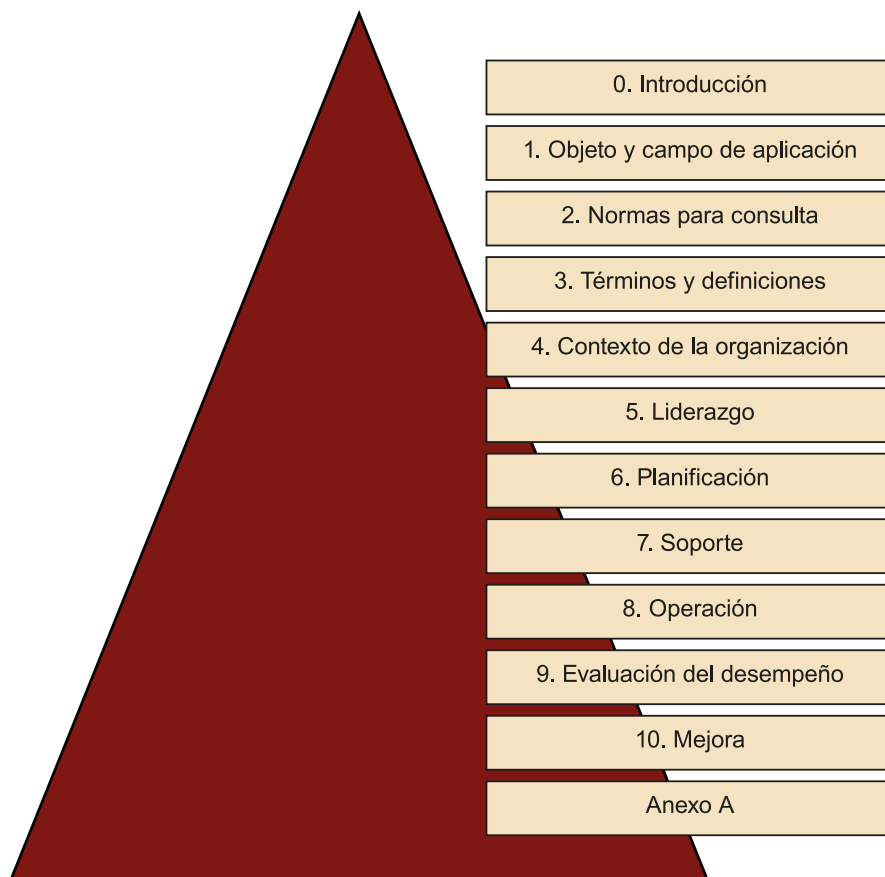
Esta estructura de la ISO/IEC 27701 se puede observar en la figura 9.

Figura 9. Estructura global de la ISO/IEC 27701



Como anteriormente hemos comentado, la ISO/IEC 27701 define los mismos requisitos que la ISO/IEC 27001, cuya estructura se puede observar en la figura 10.

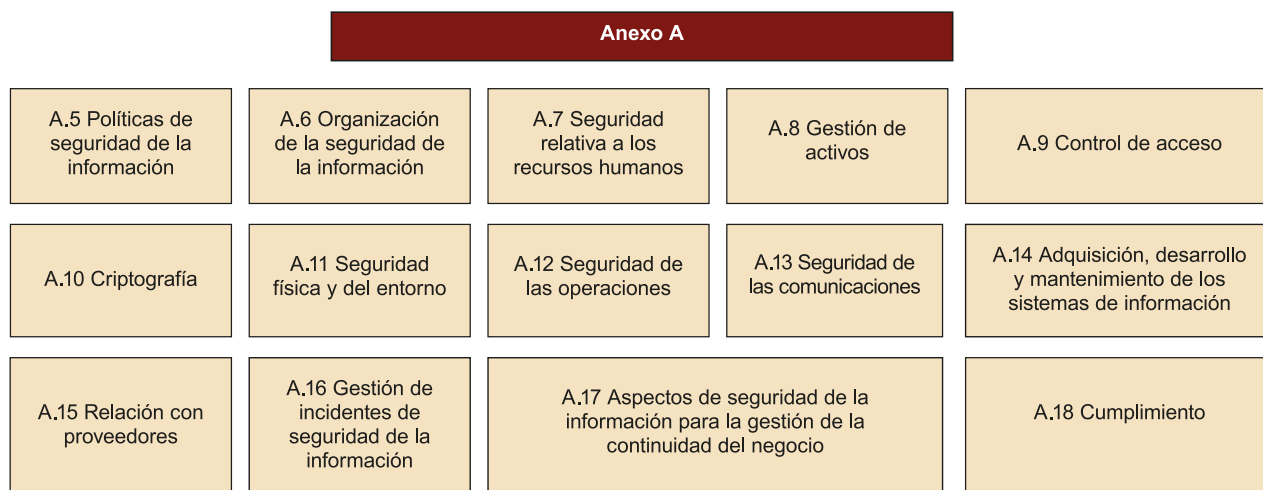
Figura 10. Estructura de la ISO/IEC 27001

**ISO/IEC 27001**

La última versión del estándar ISO/IEC 27001 es la ISO/IEC 27001:2013 y es esta versión en la que nos basamos para proporcionar la información de la figura 10.

A su vez, el anexo A de la ISO/IEC 27001 posee los grupos o dominios de controles de la figura 11.

Figura 11. Grupos de controles del anexo A de la ISO/IEC 27001



Pero la ISO/IEC 27701 no solo define los mismos requisitos que la ISO/IEC 27001, sino que utiliza los mismos controles que la ISO/IEC 27002, cuya estructura se muestra en la figura 12.

Figura 12. Estructura de la ISO/IEC 27002

**ISO/IEC 27002**

La última versión del estándar ISO/IEC 27002 es la ISO/IEC 27002:2013 y es esta versión en la que nos basamos para proporcionar la información de la figura 12.

Recordad que el anexo A de la ISO/IEC 27001 está compuesto por ciento catorce controles de seguridad y, a pesar de lo que se suele pensar, no todos son controles técnicos, sino que también existen controles organizativos o de cumplimiento, que no están directamente relacionados con las TI.

Por otra parte, como habréis podido observar, la estructura de la ISO/IEC 27001 es la misma que la estructura que comentamos en la figura 8 y la estructura de la ISO/IEC 27002 se corresponde con el contenido del anexo A de la ISO/IEC 27001.

Una vez entendidas las estructuras de las ISO/IEC 27001 y ISO/IEC 27002, podemos pasar a ver la estructura de la ISO/IEC 27701:

1. Alcance
2. Normas para consulta
3. Términos y definiciones
4. General
5. Requisitos específicos de un sistema de gestión de la información de privacidad (SGIP), relacionados con la ISO/IEC 27001

Enlace de interés

Para mayor detalle, el contenido de la ISO/IEC 27701 se puede consultar en la página oficial de iso.org: <https://www.iso.org/standard/71670.html>.

5.1. General

5.2. Contexto de la organización

5.3. Liderazgo

5.4. Planificación

5.5. Soporte

5.6. Operación

5.7. Evaluación del desempeño

5.8. Mejora

6. Guía específica de un Sistema de gestión de la información de privacidad (SGIP), relacionada con la ISO/IEC 27002

6.1. General

6.2. Políticas de seguridad de la información

6.3. Organización de la seguridad de la información

6.4. Seguridad relativa a los recursos humanos

6.5. Gestión de activos

6.6. Control de acceso

6.7. Criptografía

6.8. Seguridad física y del entorno

6.9. Seguridad de las operaciones

6.10. Seguridad de las comunicaciones

6.11. Adquisición, desarrollo y mantenimiento de los sistemas de información

6.12. Relación con proveedores

6.13. Gestión de incidentes de seguridad de la información

6.14. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

6.15. Cumplimiento

7. Guía ISO/IEC 27002 adicional para responsables de información de identificación personal

7.1. General

7.2. Condiciones para la colección y el procesamiento

7.3. Obligaciones con la información de identificación personal

7.4. Privacidad en el diseño y por defecto

7.5. Compartir, transferir y revelar información de identificación personal

8. Guía ISO/IEC 27002 adicional para encargados de información de identificación personal

8.1. General

8.2. Condiciones para la colección y el procesamiento

8.3. Obligaciones con la información de identificación personal

8.4. Privacidad en el diseño y por defecto

8.5. Compartir, transferir y revelar información de identificación personal

Anexo A. Objetivos de control y controles de referencia específicos del sistema de gestión de la información de privacidad (para responsables de información de identificación personal)

Anexo B. Objetivos de control y controles de referencia específicos del sistema de gestión de la información de privacidad (para encargados de información de identificación personal)

Anexo C. Relación con la ISO/IEC 29100

Anexo D. Relación con la regulación general de protección de datos (RGPD)

Anexo E. Relación entre ISO/IEC 27018 e ISO/IEC 29151

Anexo F. Cómo aplicar ISO/IEC 27701 a ISO/IEC 27001 e ISO/IEC 27002

Por tanto, si queremos integrar una auditoría de protección de datos con una auditoría de sistemas de información podremos usar como guía la ISO/IEC 27701, comprobando que la organización cumple con cada uno de los requisitos establecidos por este estándar.

No obstante, no debemos olvidar que la ISO/IEC 27701 está basada en la **Regulación General de Protección de Datos** (GDPR por sus iniciales en inglés, *General Data Protection Regulation*), que se desarrolló a nivel global para todos los países de la Unión Europea, aunque luego cada país miembro ha desarrollado su propia ley.

Es por ello por lo que en España tenemos la LOPD-GDD (publicada en diciembre de 2018) y aunque está basada en la regulación original, es conveniente que en las auditorías que realicemos en empresas donde se aplique la legislación española usemos también como referencia la LOPD-GDD.

2.3. Planificación, ejecución y seguimiento

Como habréis podido comprobar, realizar una auditoría de protección de datos o de sistemas de información implica revisar si la organización está cumpliendo con una serie de requisitos definidos por estándares o normativas de referencia.

Para realizar nuestro trabajo podremos basarnos en **listas de comprobación** (también conocidas como *checklists*), que nos ayudarán a determinar el nivel de cumplimiento de la organización.

Además de estas listas de comprobación, dado que hay que revisar muchos controles (en el caso del anexo A de la ISO/IEC 27001 hablamos de ciento cuarenta controles, a los que tenemos que sumar otros 49 controles específicos de la ISO/IEC 27701), puede ser interesante repartir la revisión de estos controles en diferentes auditorías.

Para ello podemos establecer una planificación, por ejemplo, a tres años, para la ejecución de la revisión de todos los controles. De esta manera, en cada auditoría podremos profundizar más intensamente en algunos grupos de controles.

No obstante, cada año deberemos revisar los principales requisitos, que básicamente son los definidos en el apartado 5 de la ISO/IEC 27701, y, por supuesto, los requisitos específicos definidos por la LOPD-GDD (recordad que para esto podéis utilizar la lista de cumplimiento de la Agencia Española de Protección de Datos).

Para poder realizar esta revisión en un plazo de tiempo determinado, es importante realizar un seguimiento en cada auditoría de los controles que ya se han revisado y de los que quedan por revisar. Para esto podéis utilizar, por ejemplo, un fichero Excel, en el que incluyáis todos los controles en filas y los años de revisión en columnas. De esta manera, podréis marcar por cada año los controles que se tendrán que revisar.

Los cambios se pueden realizar sobre la marcha, es decir, si en una auditoría no da tiempo a revisar todos los controles que estaban planificados, se pueden replanificar para la siguiente auditoría.

Suele ser recomendable revisar en cada auditoría algún control de todos los grupos de controles, por ejemplo, en el caso del anexo A de la ISO/IEC 27001, se puede revisar un control del dominio A.5, otro del A.6, otro de A.7, etc.

Es importante que la revisión que hagamos sea proporcional. Si establecemos revisar todos los controles en 3 años, cada año revisaremos un 33 %.

Por otra parte, es importante proporcionar información, en el informe de auditoría, sobre el número total de controles que se hayan podido revisar y sobre los controles que quedan pendientes.

De esta forma, la organización también podrá realizar un seguimiento sobre lo que se ha auditado y lo que todavía queda por auditar.

3. La gestión de la seguridad de la información

Hasta ahora hemos hablado mucho de requisitos, tanto de la LOPD-GDD como de la ISO/IEC 27001, pero no hemos aportado mucha información sobre estos.

En un punto anterior hemos hablado de los sistemas de gestión basados en estándares ISO. Por ejemplo, hemos hablado de forma específica de un sistema de gestión de la seguridad de la información basado en ISO/IEC 27001, que por otra parte define un modelo de mejora continua.

A lo largo de los siguientes subapartados veremos, de manera un poco más precisa, cuáles son los requisitos y los elementos más relevantes en un sistema de gestión de seguridad de la información y veremos también otras normativas relacionadas con ISO/IEC 27001 para la gestión de la seguridad.

3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2017): requisitos de sistemas de gestión de seguridad de la información, SGSI)

En el apartado 2 hemos visto cuál es la estructura de la ISO/IEC 27001 en su versión vigente (ISO/IEC 27001:2013), pero a continuación vamos a ver con más detalle los apartados de los que está compuesto este estándar, así como sus requisitos más importantes.

En primer lugar, conviene aclarar que en España tenemos la UNE ISO/IEC 27001:2017. Esto significa que existe una traducción en castellano de la ISO/IEC 27001:2013 (que se publica originalmente siempre en inglés).

Las iniciales «UNE» significan «Una Norma Española» y se añaden siempre a los estándares que se traducen al castellano.

Cada país hace lo mismo cuando traduce un estándar ISO a su idioma local, por ejemplo, en Colombia añaden «NTC» (norma técnica colombiana).

Una vez claras las diferencias, podemos continuar analizando la ISO/IEC 27001 con más detalle. Los requisitos aparecen solo entre los apartados 4 y 10, que están desarrollados en la figura 13.

Figura 13. Estructura y requisitos más relevantes de la ISO/IEC 27001:2013

4. Contexto de la organización	• Es necesario comprender la organización y su contexto (interno y externo) • Es necesario identificar las partes interesadas y conocer sus necesidades y expectativas con respecto al SGSI • Es necesario determinar los límites y el alcance del SGSI
5. Liderazgo	• Es necesario que la alta dirección demuestre su liderazgo para gestionar la seguridad de la información • Es necesario que la alta dirección se implique en el proyecto y se comprometa a proporcionar todos los recursos que sean necesarios para el SGSI • Es necesario definir una política, que tiene que estar firmada por la dirección y ser distribuida a todas las partes interesadas, o al menos estar disponible • Es necesario definir roles y responsabilidades para el SGSI
6. Planificación	• Es necesario identificar riesgos y evaluarlos. La identificación y evaluación de estos riesgos tiene que realizarse de acuerdo a una metodología de gestión de riesgos • Es necesario definir objetivos de seguridad de la información, los cuales tienen que estar aprobados por la alta dirección
7. Soporte	• Es necesario establecer recursos para el SGSI • Es necesario definir las competencias de cada una de las personas implicadas en el SGSI (alta dirección, responsable de seguridad, auditor interno, consultor, responsable sistemas, desarrolladores, etc.) • Es necesario establecer planes para concienciar al personal en materia de seguridad de la información • Es necesario establecer canales para los comunicados internos y externos relativos al SGSI (quién, cómo, cuándo, qué) • Es necesario gestionar la información documentada, estableciendo dónde se almacenará, cómo se versionará, cómo se gestionarán documentos obsoletos, documentos externos, etc.
8. Operación	• Es necesario llevar a cabo un tratamiento de los riesgos identificados e implementar un plan de tratamiento de riesgos
9. Evaluación del desempeño	• Es necesario establecer un método para realizar un seguimiento, medición, análisis y evaluación del SGSI (habitualmente métricas) • Es necesario llevar a cabo una auditoría interna, que tiene que ser llevada a cabo por personal independiente al SGSI • Es necesario llevar a cabo la revisión por dirección, en la que la dirección revisará los elementos más relevantes del SGSI
10. Mejora	• Es necesario establecer un método para el tratamiento de las desviaciones detectadas, para el que se implementarán acciones correctivas • Es necesario demostrar que el SGSI se mejora de manera continua

Es importante también destacar que este estándar obliga a que existan un mínimo de documentos en el SGSI, los cuales se detallan a continuación:

- **Alcance del SGSI:** debe indicar información precisa acerca del contexto, las partes interesadas, infraestructura tecnológica, legislación aplicable, sistemas de información implicados, áreas, servicios, procesos, etc.
- **Política de seguridad de la información:** es una declaración de intenciones, donde la organización establece su compromiso para cumplir con los requisitos aplicables a la seguridad de la información.
- **Objetivos de seguridad de la información:** debe indicar cuáles son los objetivos de la organización para la implementación del SGSI, los cuales deben ser específicos para el negocio, y se debe establecer un método para saber si se consiguen o no. Por tanto, estos objetivos de seguridad tienen que estar alineados con el negocio y ayudar a mejorar el SGSI.
- **Metodología de gestión de riesgos:** debe indicar el proceso completo que sigue la organización para la identificación, evaluación y tratamiento de

los riesgos. Además, debe existir información documentada sobre los resultados del análisis de riesgos, así como del Plan de Tratamiento de Riesgos.

- **Declaración de aplicabilidad:** debe indicar, para cada uno de los controles del anexo A de la ISO/IEC 27001, cuáles aplican o no, justificando para cada control el porqué.
- **Definición de roles y responsabilidades:** debe indicar los diferentes roles que se establecen en el SGSI, así como sus respectivas responsabilidades.
- **Registros de formación:** es necesario que la organización conciencie al personal en materia de seguridad de la información y demuestre, por ejemplo, con registros de asistencia, que el personal ha sido concienciado.
- **Resultados de monitorización del SGSI:** es necesario que la organización demuestre que está monitorizando y midiendo el SGSI, por ejemplo, usando métricas.
- **Programa de auditoría interna y resultados:** es necesario que la organización demuestre que realiza auditorías internas, por ejemplo, con el informe de auditoría, que indique los resultados de la misma. También debe demostrar que tiene un programa para realizar sus auditorías internas (anual o semestral), que incluya la revisión de todos los requisitos y controles.
- **Resultados de la revisión por dirección:** es necesario que la organización demuestre que realiza la revisión por dirección, por ejemplo, a través de un acta de una reunión en la que se puedan comprobar los participantes, los puntos revisados, la fecha, etc.
- **Resultados de acciones correctivas:** es necesario que la organización posea un método para el tratamiento de las desviaciones, por ejemplo, con el registro de acciones correctivas definidas para cada una de las desviaciones.

Además, para la parte de los controles, el estándar establece que la organización tiene que tener información documentada para los siguientes controles:

- A.8.1.1 Inventario de activos
- A.8.1.3 Uso aceptable de los activos
- A.9.1.1 Política de control de acceso
- A.12.1.1 Procedimientos de operación para la gestión de TI
- A.14.2.5 Principios de ingeniería de sistemas seguros
- A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores
- A.16.1.5 Respuesta a incidentes de seguridad de la información

- A.17.1.2 Implementación de la continuidad de la seguridad de la información
- A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Una vez clara la estructura de la ISO/IEC 27001, vamos a conocer otra normativa relacionada con la gestión de la seguridad de la información, muy relevante en España, dado que es obligatoria en determinados entornos.

Esta normativa de la que hablamos se trata del **Esquema Nacional de Seguridad**, y posee muchos puntos en común con la ISO/IEC 27001. Aunque persiguen objetivos distintos, la esencia de ambos es la misma: proteger la información.

El Centro Criptológico Nacional define el esquema nacional de seguridad (ENS) de la siguiente manera:

«La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos estableció el esquema nacional de seguridad que, aprobado mediante Real decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, recoge el esquema nacional de seguridad en su artículo 156 apartado 2 en similares términos.

En 2015 se publicó la modificación del esquema nacional de seguridad a través del Real decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del esquema».

Por tanto, a grandes rasgos, vemos que el ENS es una ley que se aplica al sector público, es decir, a las administraciones públicas (ayuntamientos, universidades, etc.), y tiene como principal objetivo proteger la información. En este caso se refiere al acceso a través de internet que los ciudadanos tienen de la información electrónica que las administraciones públicas gestionan.

En definitiva, el esquema nacional de seguridad establece una serie de requisitos, que las entidades obligadas a cumplir con este ENS tienen que implementar. Estos requisitos vienen claramente definidos en el ENS, el cual está compuesto de 44 artículos y 5 anexos.

Una de las diferencias más destacables entre la estructura del ENS y la del ISO/IEC 27001, es que la ISO/IEC 27001, como ya sabemos, establece unos requisitos mínimos que una organización tiene que tener para definir un SGSI.

Sin embargo, el ENS, en algunos casos específicos, habla de que es necesario un SGSI, pero no establece requisitos.

Enlace de interés

Se puede acceder al contenido completo del ENS, de manera gratuita en el siguiente enlace: <https://www.boe.es/eli/es/rd/2010/01/08/3/con>.

Otra diferencia importante es que en la ISO/IEC 27001 tenemos que llevar a cabo un análisis de riesgos y, después de este, seleccionar los controles del anexo A que necesitemos para tratar los riesgos identificados.

En el caso del ENS, tenemos que categorizar los sistemas de información, los cuales pueden clasificarse de acuerdo a tres categorías:

- básica,
- media,
- alta.

Cuanto mayor sea la categoría, mayor será el número de medidas de seguridad a implementar.

De esta manera, si la categoría del sistema es básica, se aplicarán solo las medidas de seguridad que corresponden a esta categoría. Si la categoría del sistema es media, se aplicarán las medidas de seguridad que corresponden a la categoría básica y a la categoría media. Y si la categoría del sistema es alta, se aplicarán todas las medidas de seguridad (categorías básica, media y alta).

Por otra parte, para determinar la categoría del sistema de información es necesario evaluar la seguridad en cada una de las dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad). De acuerdo a esta evaluación, el nivel para cada dimensión puede ser bajo, medio o alto.

En el anexo I del ENS se establecen los siguientes criterios para la determinación del nivel en una dimensión de seguridad y de la categoría del sistema:

- Un sistema de información será de categoría alta si alguna de sus dimensiones de seguridad alcanza el nivel alto.
- Un sistema de información será de categoría media si alguna de sus dimensiones de seguridad alcanza el nivel medio, y ninguna alcanza un nivel superior.
- Un sistema de información será de categoría básica si alguna de sus dimensiones de seguridad alcanza el nivel bajo, y ninguna alcanza un nivel superior.

Con respecto a las medidas de seguridad del ENS, vienen definidas en el anexo II, y están organizadas en diferentes grupos:

1) Marco organizativo

- org.1 Política de seguridad
- org.2 Normativa de seguridad

- org.3 Procedimientos de seguridad
- org.4 Proceso de autorización

2) Marco operacional

a) Planificación

- op.pl.1 Análisis de riesgos
- op.pl.2 Arquitectura de seguridad
- op.pl.3 Adquisición de nuevos componentes
- op.pl.4 Dimensionamiento/Gestión de capacidades
- op.pl.5 Componentes certificados

b) Control de acceso

- op.acc.1 Identificación
- op.acc.2 Requisitos de acceso
- op.acc.3 Segregación de funciones y tareas
- op.acc.4 Proceso de gestión de derechos de acceso
- op.acc.5 Mecanismo de autenticación
- op.acc.6 Acceso local
- op.acc.7 Acceso remoto

c) Explotación

- op.exp.1 Inventario de activos
- op.exp.2 Configuración de seguridad
- op.exp.3 Gestión de la configuración
- op.exp.4 Mantenimiento
- op.exp.5 Gestión de cambios
- op.exp.6 Protección frente a código dañino
- op.exp.7 Gestión de incidentes
- op.exp.8 Registro de la actividad de los usuarios
- op.exp.9 Registro de la gestión de incidentes
- op.exp.10 Protección de los registros de actividad
- op.exp.11 Protección de claves criptográficas

d) Servicios externos

- op.ext.1 Contratación y acuerdos de nivel de servicio
- op.ext.2 Gestión diaria
- op.ext.9 Medios alternativos

e) Continuidad del servicio

- op.cont.1 Análisis de impacto
- op.cont.2 Plan de continuidad

- op.cont.3 Pruebas periódicas

f) Monitorización del sistema

- op.mon.1 Detección de intrusión
- op.mon.2 Sistema de métricas

3) Medidas de protección

a) Protección de las instalaciones e infraestructuras

- mp.if.1 Áreas separadas y con control de acceso
- mp.if.2 Identificación de las personas
- mp.if.3 Acondicionamiento de los locales
- mp.if.4 Energía eléctrica
- mp.if.5 Protección frente a incendios
- mp.if.6 Protección frente a inundaciones
- mp.if.7 Registro de entrada y salida de equipamiento
- mp.if.9 Instalaciones alternativas

b) Gestión de personal

- mp.per.1 Caracterización del puesto de trabajo
- mp.per.2 Deberes y obligaciones
- mp.per.3 Concienciación
- mp.per.4 Formación
- mp.per.9 Personal alternativo

c) Protección de los equipos

- mp.eq.1 Puesto de trabajo despejado
- mp.eq.2 Bloqueo de puesto de trabajo
- mp.eq.3 Protección de equipos portátiles
- mp.eq.9 Medios alternativos

d) Protección de las comunicaciones

- mp.com.1 Perímetro seguro
- mp.com.2 Protección de la confidencialidad
- mp.com.3 Protección de la autenticidad y de la integridad
- mp.com.4 Segregación de redes
- mp.com.9 Medios alternativos

e) Protección de los soportes de información

- mp.si.1 Etiquetado
- mp.si.2 Criptografía

- mp.si.3 Custodia
- mp.si.4 Transporte
- mp.si.5 Borrado y destrucción

f) Protección de las aplicaciones informáticas

- mp.sw.1 Desarrollo
- mp.sw.2 Aceptación y puesta en servicio

g) Protección de la información

- mp.info.1 Datos de carácter personal
- mp.info.2 Calificación de la información
- mp.info.3 Cifrado
- mp.info.4 Firma electrónica
- mp.info.5 Sellos de tiempo
- mp.info.6 Limpieza de documentos
- mp.info.9 Copias de seguridad

h) Protección de los servicios

- mp.s.1 Protección del correo electrónico
- mp.s.2 Protección de servicios y aplicaciones web
- mp.s.8 Protección frente a la denegación de servicio
- mp.s.9 Medios alternativos

Si os fijáis en estas medidas de seguridad, que en total son setenta y cinco, algunas os sonarán del anexo A de la ISO/IEC 27001: org.1 Política de seguridad, op.pl.1 Análisis de riesgos, etc.

También podéis comprobar que existe una medida específica para la protección de datos personales: mp.info.1 Datos de carácter personal

Aunque en este caso el ENS hace referencia a la antigua LOPD, es decir, no está actualizado con la nueva LOPD-GDD, simplemente habrá que establecer un control para cumplir con la LOPD-GDD actual.

En definitiva, podéis ver que hay una relación estrecha entre ISO/IEC 27001 y el ENS, a pesar de sus diferencias.

Muchas organizaciones utilizan la base de la ISO/IEC 27001 para establecer el sistema de gestión de seguridad de la información y, a partir de ahí, implementan las medidas de seguridad que sean necesarias, tanto por parte de la ISO/IEC 27001, como de la LOPD-GDD, como del ENS.

3.2. Gestión de la seguridad de los activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación

Cuando hablamos de medidas de seguridad específicas de la ISO/IEC 27001, hasta ahora solo hemos hablado de dominios o grupos de controles, pero no hemos visto los controles de seguridad específicos del anexo A de la ISO/IEC 27001. Veamos por tanto a continuación el listado completo:

A.5 Políticas de seguridad de la información

- A.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

- A.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
- A.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

- A.7.1 Antes del empleo
 - A.7.1.1 Investigación de antecedentes
 - A.7.1.2 Términos y condiciones del empleo
- A.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

Enlace de interés

Existe una guía, desarrollada por el Centro Criptológico Nacional, en la que se establece una relación entre la ISO/IEC 27001, la ISO/IEC 27002 y el ENS. Esta guía es la «CCN-STIC-825» y podéis encontrarla de forma gratuita aquí: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html>.

- A.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

- A.8.1 Responsabilidades 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
- A.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 Manipulación de la información
- A.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

- A.9.1 Requisitos de 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
- A.9.2 Gestión de acceso de usuario
 - A.9.2.1 Registro y baja de usuario
 - 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 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
- A.9.3 Responsabilidades del usuario
 - A.9.3.1 Uso de la información secreta de autenticación
- A.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 privilegios del sistema

- A.9.4.5 Control de acceso al código fuente de los programas

A.10 Criptografía

- A.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 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 equipos
 - 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 y 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 del software en explotación
- A.12.6 Gestión de la vulnerabilidad técnica
 - A.12.6.1 Gestión de las vulnerabilidades técnicas
 - A.12.6.2 Restricción 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 electrónica
 - 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 sistemas
 - 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 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 de sistemas
 - A.14.2.9 Pruebas de aceptación de sistemas
- A.14.3 Datos de prueba
 - A.14.3.1 Protección de los datos de prueba

A.15 Relación con proveedores

- A.15.1 Seguridad en las relaciones con 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
- A.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 de 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 la seguridad
 - A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la 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 Implementación de 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
 - 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
- A.18.2 Revisiones de la seguridad de la información
 - A.18.2.1 Revisión independiente de la seguridad de la información
 - A.18.2.2 Cumplimiento de las políticas y normas de seguridad
 - A.18.2.3 Comprobación del cumplimiento técnico

De todos estos controles (ciento catorce en total), vamos a centrarnos en los relacionados con la gestión de la seguridad de los activos, la seguridad lógica y la seguridad de las TI, dado que estos grupos de controles suelen generar ciertas dudas.

En primer lugar, con respecto a los controles relacionados con la **gestión de la seguridad de los activos**, tenemos el dominio «A.8 Gestión de activos», compuesto a su vez por tres objetivos de control:

- A.8.1 Responsabilidades sobre los activos
- A.8.2 Clasificación de la información
- A.8.3 Manipulación de los soportes

Aparte, como ya sabemos, para cada objetivo de control, a su vez se definen controles de seguridad (A.8.1.1 Inventario de activos, A.8.1.2 Propiedad de los activos, etc.).

Hasta aquí todo está muy claro, pero nos falta definir de forma precisa qué puede ser un **activo**. Un activo es «cualquier cosa que tenga valor para la organización».

Por tanto, pueden existir multitud de activos que la organización debe haber identificado.

Para realizar este ejercicio de identificación de activos, lo habitual es definir diferentes categorías y, por cada una, pensar qué activos pueden existir en la organización.

Las categorías más habituales son las siguientes:

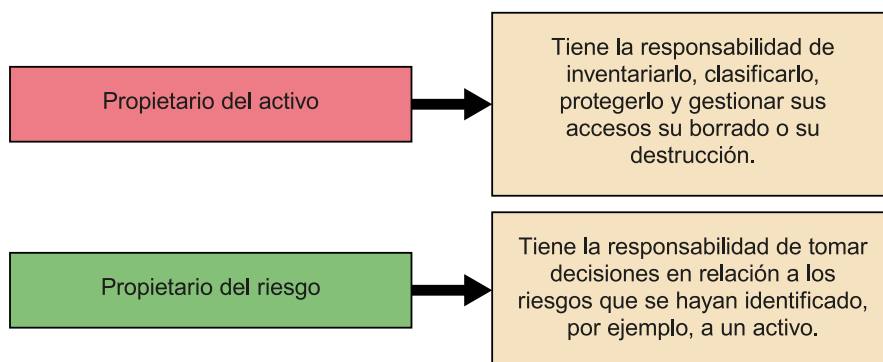
- **Información:** clientes, proveedores, etc.
- **Hardware:** equipos de sobremesa, portátiles, etc.
- **Software:** sistema operativo, paquete ofimático, etc.
- **Redes:** *routers*, puntos de acceso, etc.
- **Personal:** alta dirección, responsable de proyecto, técnicos, etc.
- **Locales:** oficina, CPD, etc.
- **Servicios:** limpieza, seguridad física instalaciones, etc.

Enlace de interés

Existe un estándar ISO que nos puede ayudar a identificar activos, que es la ISO/IEC 27005, que se puede descargar con previo pago de la siguiente dirección: <https://www.iso.org/standard/75281.html>.

Asimismo, es importante saber diferenciar entre el **propietario del activo** (control A.8.1.2) y el **propietario del riesgo**. Esta diferencia se muestra en la figura 14.

Figura 14. Diferencias entre el propietario del activo y el propietario del riesgo



En segundo lugar, con respecto a los controles relacionados con la **seguridad lógica**, tenemos el dominio de controles «A.9 Control de acceso», compuesto por cuatro objetivos de control:

- A.9.1 Requisitos de negocio para el control de acceso
- A.9.2 Gestión de acceso de usuario
- A.9.3 Responsabilidades del usuario
- A.9.4 Control de acceso a sistemas y aplicaciones

Las organizaciones suelen implementar este grupo de controles a través de sistemas de gestión de usuario, como por ejemplo, el Directorio Activo en entornos Windows, o el OpenLDAP, o similares, en entornos Linux.

No obstante, dentro de este grupo de controles, se puede considerar cualquier gestión de accesos que se utilice en la organización, incluyendo accesos a la red wifi, accesos a servicios en la nube (AWS, Azure, etc.), accesos locales a equipos fuera de dominio, accesos a sistemas que no integran la autenticación con el directorio activo, etc.

También es importante saber que, aunque el estándar no define una longitud mínima específica para las contraseñas de los accesos de los usuarios, es recomendable establecer, como mínimo, ocho caracteres y la contraseña debe ser intransferible.

También se pueden utilizar gestores de contraseñas, pero en este caso, dado que existen muchas herramientas en el mercado, es necesario realizar un estudio detallado de beneficios/desventajas que proporciona cada una, dado que estas herramientas pueden llegar a almacenar información muy sensible de la organización.

Por último, con respecto a los controles relacionados con la **seguridad de las TI**, los grupos de controles que nos pueden ayudar son los de los dominios:

- **A.12 Seguridad de las operaciones:** dispone de controles específicos para documentar procedimientos de operación de sistemas (servidores, conexiones remotas), gestionar la capacidad (recursos de memoria, CPU, etc.), gestión de cambios (cómo se solicitan, quién los aprueba, etc.), gestión de *malware*, copias de seguridad, vulnerabilidades técnicas (*hacking* ético, *pentesting*, etc.), gestión de logs, separación de entornos (desarrollo, prueba y producción), control del paso a producción, etc.
- **A.13 Seguridad de las comunicaciones:** dispone de controles específicos para gestionar los accesos a la red (cableada o inalámbrica), segmentar la red, gestionar la seguridad de los servicios de red, gestionar acuerdos de intercambio de información, correo electrónico, etc.

En relación con las TI, existe también el dominio «A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información», que se suele asociar al desarrollo de software, aunque dentro de este dominio existen algunos controles que no son para eso. En concreto, hablamos de los tres controles que componen el objetivo de control «A.14.1. Requisitos de seguridad en sistemas de información».

Los que sí tienen una relación directa con el desarrollo software son los nueve controles del objetivo de control «A.14.2. Seguridad en el desarrollo y en los procesos de soporte».

Por tanto, una empresa que no desarrolle software podría decidir establecer como no aplicables todos los controles del objetivo de control A.14.2.

Con respecto al control «A.14.3.1. Protección de los datos de prueba», no es necesario que la organización desarrolle software para que aplique, dado que se refiere a pruebas que se realicen con datos reales.

Por ejemplo, podemos imaginar que la organización no desarrolla software, pero tiene un fichero Excel para tratar información de sus clientes. Para probar el funcionamiento de este fichero Excel, se debe evitar usar datos reales, porque se podría vulnerar su privacidad. Por tanto, en este caso, los controles del A.14.2 podrían establecerse como no aplicables y los del A.14.3.1 sí que se podrían aplicar.

Con respecto a todos los controles que hemos visto relacionados con las TI, tenemos que tener en cuenta que actualmente, y cada vez más, muchas empresas tienden a externalizar el área de TI. En esos casos, podemos encontrarnos con que controles relativos a TI se delegan a un proveedor o directamente el riesgo se transfiere a esta.

En cualquier caso, la responsabilidad de los controles seguirá siendo de la organización, por lo que tendrá que supervisarlos y, cuando sea posible, también podría auditarlos, para de esta manera comprobar su adecuada implementación.

3.3. Recuperación ante desastres y continuidad del negocio.

Protección de los activos técnicos y documentales.

Planificación y gestión de la recuperación ante desastres

Otro de los grupos de controles importantes del anexo A de la ISO/IEC 27001 es el «A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio», el cual proporciona controles para que el negocio, en caso de interrupción, pueda seguir funcionando.

Se pueden diferenciar dos escenarios:

- Continuidad de las TI y los sistemas de información.
- Continuidad de todas las actividades, procesos, áreas, etc. del negocio.

Para el primer escenario, se suele hablar de **planes de recuperación ante desastres**, que están más enfocados a recuperar el funcionamiento de la infraestructura tecnológica.

Para el segundo escenario, se suele hablar de **planes de continuidad del negocio**, que están enfocados a recuperar el funcionamiento de todo el negocio, incluyendo también toda la parte de TI. Por tanto, un plan de continuidad del negocio también podría contener un plan de recuperación ante desastres.

Por otra parte, dado que el objetivo principal de la ISO/IEC 27001 es la protección de la información y esta suele encontrarse principalmente en activos, que pueden ser sistemas de información, a la hora de abordar los controles del A.17 podremos pensar en un plan de recuperación ante desastres.

A la hora de desarrollar un plan de recuperación ante desastres, es necesario considerar dos etapas principales:

- **Respuesta:** se produce la parada de la infraestructura tecnológica y es necesario proporcionar una alternativa rápida para que el negocio siga funcionando. Por ejemplo, si se cae el CPD principal, puede entrar en funcionamiento un CPD alternativo.
- **Recuperación:** en esta etapa estaremos funcionando con el CPD alternativo, pero las opciones alternativas generalmente están pensadas para funcionar de manera temporal y en algunos casos puede que el funcionamiento sea degradado mientras se recupera el entorno principal. Por tanto, una vez que el CPD principal esté operativo, en esta etapa se inician las actividades de recuperación para volver al 100 % del funcionamiento normal.

Por otra parte, también es necesario considerar cuáles pueden ser los escenarios más probables que pueden provocar una interrupción, como por ejemplo:

- El sistema de información específico del CPD deja de funcionar.
- Los sistemas de información del CPD dejan de funcionar.
- Falla el suministro eléctrico y se apaga todo el CPD.
- Un desastre natural provoca la destrucción del CPD y de las instalaciones donde se encuentra la organización.
- El personal crítico de la organización se ausenta en su puesto de trabajo (por huelga, enfermedad, etc.).

Cada uno de estos escenarios, en mayor o menor medida, puede provocar una interrupción, por lo que se deben establecer para cada uno acciones de contingencia, en otras palabras, acciones que establece la organización para dar respuesta y recuperar el negocio ante cada una de estas situaciones.

Por otra parte, es importante planificar la realización de pruebas de cada uno de estos escenarios. Las pruebas no tienen que ser reales, pero se pueden hacer simulaciones. Tampoco es necesario probar todos los escenarios el mismo año, sino que se puede programar su ejecución en un plazo de tiempo, de forma que se puedan probar todos los escenarios identificados.

Como resultado de las pruebas, es importante dejar algún registro como evidencia de su ejecución, por ejemplo, en forma de informe, con el detalle de las pruebas realizadas, los tiempos necesarios para su ejecución, el personal que ha participado, los recursos utilizados, etc.

Resumen

A lo largo de este módulo hemos visto un método básico para llevar a cabo auditorías de protección de datos, definiendo los pasos del proceso completo, compuesto principalmente por tres etapas:

- **Preauditoría:** se selecciona a las personas que formarán parte del equipo auditor, se acuerda con la organización las fechas y los horarios para llevar a cabo la auditoría y se hace una revisión previa, en remoto, de la documentación que tenga la organización relativa a la normativa de referencia
- **Auditoría:** se lleva a cabo la auditoría, considerando la revisión de los principios y los requisitos de la normativa de referencia. Para esta revisión, es necesario mantener reuniones con el personal y siempre se debe establecer una reunión inicial de apertura, para presentar a la organización el proceso, y otra reunión de cierre, para proporcionar las conclusiones finales. Cuando la auditoría tenga una duración de varios días, al final de cada día, se realizará también una reunión de *feedback* para mantener informada a la organización, de manera continua, sobre los hallazgos que se vayan detectando.
- **Posauditoría:** se elabora el informe final y se entrega a la organización. Como el informe contendrá hallazgos, la organización tiene que tratarlos y presentar evidencias de las acciones que haya llevado a cabo para el tratamiento.

También hemos visto el tipo de hallazgos que se pueden determinar durante una auditoría, que básicamente podemos identificar en:

- **No conformidades** (mayores o menores, dependiendo de la criticidad).
- **Observaciones** (no son incumplimientos, pero si no se tratan, en el futuro se pueden convertir en no conformidad).
- **Oportunidades de mejora** (solo son recomendaciones del equipo auditor).

Adicionalmente hemos visto la diferencia entre las auditorías de protección de datos y las auditorías de los sistemas de información, y hemos visto cómo se pueden integrar.

También hemos introducido la **ISO/IEC 27701**, que básicamente es un estándar internacional que une requisitos de la ISO/IEC 27001 con el RGPD.

Además, hemos visto las diferencias entre la ISO/IEC 27001, su anexo A y la ISO/IEC 27002, viendo un poco más en detalle ciertos dominios de controles para la gestión de activos, el control de acceso, la seguridad de las operaciones, la seguridad de las redes y la continuidad de negocio.

Otra normativa, relacionada con la seguridad de la información, que también hemos visto durante el estudio de este módulo, ha sido el **Esquema Nacional de Seguridad** (ENS), conociendo los diferentes niveles que se pueden certificar, así como las medidas de seguridad que establece para la protección de la seguridad de la información, teniendo relación tanto con la ISO/IEC 27001 como con la LOPD.

Bibliografía

General Data Protection Regulation <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>>

ISO/IEC 27001:2013 Information Security Management <<https://www.iso.org/iso-iec-27001-information-security.html>>

ISO/IEC 27002:2013 Code of Practice for Information Security controls <<https://www.iso.org/standard/54533.html>>

ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management <<https://www.iso.org/standard/71670.html>>

ISO 19011:2018 Guidelines for Auditing Management systems <<https://www.iso.org/standard/70017.html>>

Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales <<https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>>

Ley orgánica 15/1999, de 13 de diciembre, de protección de datos personales <<https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>>

Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica <<https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330>>

