# Entorno de mantenimiento y conservación de documentos electrónicos

Carlota Bustelo Ruesta

PID_00202267

UOC
Universitat Oberta de Catalunya

# Índice

# Introducción

En este módulo vamos a identificar los distintos entornos donde se mantienen y conservan los documentos electrónicos en las organizaciones. Describimos las situaciones más habituales a la hora de hacer el análisis de contexto organizativo, necesario para la implantación de un modelo de gestión documental.

Además, vamos a acercarnos a las tecnologías de la información y a las infraestructuras de la organización que estamos analizando para entenderlas desde una perspectiva global. Ello nos permitirá realmente comprender los entornos de mantenimiento y conservación de documentos electrónicos.

Por esta razón haremos especial hincapié en las políticas de seguridad de la información, que describiremos a grandes rasgos en relación con la gestión de los documentos. Entender estas políticas y cómo se aplican en la organización en concreto es una parte importante del análisis de contexto.

# Objetivos

**1.** Aprender a identificar los distintos entornos en los que se mantienen y conservan los documentos electrónicos en las organizaciones.

**2.** Identificar las tecnologías de la información y sus infraestructuras existentes en la organización.

**3.** Conocer las políticas de seguridad de la información y cómo se aplican.

# 1. Entendimiento de la arquitectura y sistemas de información

Los documentos electrónicos son parte de la información que se maneja en los sistemas de información de cualquier organización. Para completar el análisis del contexto organizativo, hay que entender cómo se organiza la información en la organización y si existen algunas políticas que pueden influir o condicionar la gestión de los documentos electrónicos.

En muchas organizaciones pequeñas o medianas puede faltar una implantación consciente de una determinada arquitectura de información. En las organizaciones grandes lo normal es que exista un **plan de sistemas de información** que dirija la implantación de tecnologías de la información, tanto de hardware como de software.

Entender estos condicionantes es imprescindible para poder proponer cómo implantar soluciones de gestión de los documentos electrónicos, que en la mayoría de los casos supondrá la incorporación de un software específico para su gestión. Este deberá incorporarse a la arquitectura ya existente en la organización, o proponer cambios justificados de dicha arquitectura mediante una inversión razonable.

El primer paso, por lo tanto, para analizar el entorno de mantenimiento y conservación de los documentos electrónicos es estudiar, si los hubiera, los documentos que definen la arquitectura de información, el plan de sistemas o cualquier otro documento relacionado con los sistemas de información de la organización.

# 2. El almacenamiento en ordenadores y redes

En el análisis del entorno de conservación y preservación, es importante identificar los ordenadores y las redes que forman parte del sistema de información de la organización, en la cual hemos de definir políticas de gestión documental.

Los aspectos que hemos de analizar concretamente son:

- Cómo están organizados los ficheros identificados como documentos.
- Si se almacenan documentos en los discos duros de los ordenadores personales.
- Si hay servidores de ficheros y datos y cómo son.
- Si se está almacenando en la nube, *off-line, near-line*.
- Cómo se gestiona la documentación de y en correo electrónico.

## 2.1. Organización de ficheros identificados como documentos

Los sistemas de información requieren para su funcionamiento el almacenamiento de gran cantidad de ficheros de distintos tipos que permiten el funcionamiento del hardware, el software y las comunicaciones. De entre estos ficheros tenemos los concernientes a los sistemas operativos, dispositivos, seguridad y gestión de usuarios. Además existen los ficheros que componen las distintas aplicaciones de software o programas.

La organización de todos estos ficheros es tarea de los administradores de redes y sistemas informáticos, y dependerá en gran parte de los sistemas operativos, los dispositivos instalados, la estructura de las redes y los servidores y la definición de usuarios.

De todos estos ficheros, desde el punto de vista de la gestión de los documentos, lo que nos interesa son los ficheros de usuario o los generados con los datos e información que provienen de las actividades realizadas.

No existen unos principios de organización universales para este tipo de ficheros. Dependiendo de la complejidad de la organización, estos ficheros pueden encontrarse almacenados de distintas formas.

### 2.1.1. El almacenamiento en discos duros de los ordenadores personales

En organizaciones pequeñas y poco estructuradas es normal que los ficheros de datos se encuentren en los discos duros de los ordenadores personales siguiendo los propios criterios de las personas que los usan. Esto ocurre a ve-

ces aunque los ordenadores se encuentren en red y se compartan aplicaciones de gestión. De hecho, el sistema operativo Windows, el más extendido para los ordenadores personales, ya propone por defecto que la ubicación de los ficheros que se producen con las herramientas de edición de documentos sea un directorio llamado "Mis documentos". Esta forma de almacenamiento de ficheros tiene grandes desventajas en cuanto a:

- Acceso a los documentos, ya que para que otras personas accedan a los mismos deben convertirse las carpetas en compartidas de manera intencionada por el usuario del ordenador.

- Gestión de las copias de seguridad que no pueden hacerse de forma centralizada.

- Cantidad de duplicados que produce la filosofía de que los documentos son propios de cada persona y no son documentos o información corporativos.

Por eso es muy habitual que las organizaciones pasen rápidamente a un sistema de servidores de ficheros y datos.

### 2.1.2. Servidores de ficheros y datos

En distintas configuraciones de ordenadores en red, se permite acotar un determinado espacio de alguno de los servidores para que sea el lugar de almacenamiento de los ficheros de usuario.

La idea principal es mantener todos los ficheros de datos en una misma ubicación de manera que permita la actuación y la aplicación de determinadas medidas, de una manera más fácil y corporativa.

Aunque este es un paso importante para la consideración de la información y los documentos como corporativos y no "personales", en la organización más clásica de unidades de red y directorios se mantienen también los espacios personales.

En unos apuntes clásicos para configuración de carpetas compartidas podemos encontrar algunas sugerencias y modelos de organización de carpetas compartidas (González).

**Lectura recomendada**

Curso en línea. Trabajo colaborativo apoyado en la red, por Víctor R. González Fernández para la Inspección de Educación de Castilla y León http://platea.pntic.mec.es/vgonzale/trabcolab_0910/index.htm

Según este texto los principales modelos para organizar la información en carpetas compartidas son:

- **Jerárquico**: En el que la información y los permisos de acceso a ella estarían distribuidos según las diferentes unidades de la organización. La organización contaría con una macrocarpeta compartida, en la que, a su vez, existirían tantas subcarpetas compartidas como secciones tenga, y quizá

algunas más con el objeto de dar soporte al trabajo intersecciones. Los trabajadores tendrían acceso a la carpeta de su sección y a alguna de las subcarpetas de soporte.

- **Temático**: Se contaría con una carpeta compartida para cada tema abordado por la organización. Un trabajador tendría acceso a tantas carpetas compartidas como temas sean de su competencia. Asimismo, probablemente tendría acceso a algunas otras carpetas de soporte y recursos, y con un nivel de permisos de acceso que depende de su cargo.

- **Por procesos**: Distribución análoga a la temática pero con un enfoque basado en el trabajo por procesos.

- **Mixto**: Distribución híbrida de las anteriores.

Un modelo que se ha impuesto en muchas organizaciones que intentan hacer desaparecer información relevante de los discos duros de los ordenadores personales es la división del almacenamiento en diferentes unidades de red, que se definen por los permisos de acceso.

- En este espacio común cada usuario tiene un espacio al que solo tiene acceso él mismo, y que sustituye a su disco duro.

- Existen diferentes unidades jerárquicas que representan grupos de trabajo o unidades organizativas a las que acceden todos los usuarios que la conforman.

Cuando se produce esta organización de las unidades de red, para poder analizar el entorno de mantenimiento y conservación de los documentos tendremos que tratar de analizar cómo son los comportamientos de las personas con respecto a esta organización, y cómo están definidos los permisos para hacer ciertas acciones. Concretamente nos fijaremos en los siguientes aspectos:

- Si existen criterios de cuáles son los documentos que se deben integrar en uno u otro nivel y si están recogidos en algún documento que se va actualizando.

- Si los documentos se "mueven" de un directorio a otro o se "copian", quién lo hace y si hay procedimientos establecidos.

- Cómo se vacían los directorios cuando alcanzan su nivel máximo de almacenamiento, quién lo hace, y si dicho vaciado está procedimentado.

## 2.2. El almacenamiento en la nube

La nube o el *cloud computing* es importante desde el punto de vista del entorno de producción de los documentos electrónicos, pero este tipo de servicios también tiene un componente importante cuando queremos analizar el entorno de mantenimiento y conservación de los documentos.

Quizás no haya pasado mucho tiempo en el uso de servicios de este tipo para sacar conclusiones acertadas sobre el impacto de esta tecnología en el mantenimiento y conservación de los documentos electrónicos. No obstante, teniendo en cuenta los objetivos de cualquier sistema de gestión de documentos y sus objetivos, podemos tomar en consideración algunas reflexiones cuando el almacenamiento en la nube es el planteamiento de las organizaciones. En este sentido cabría preguntarse:

- ¿Es el almacenamiento en la nube una solución para el mantenimiento y conservación de la información y los documentos?
- ¿Se han establecido plazos para que una información siga almacenada en estos servicios?
- ¿Se ha contratado un espacio que puede crecer indefinidamente?
- ¿Se ha de mantener una copia local de todo lo que está en la nube?
- ¿Se han incluido en los contratos de servicios qué es lo que sucede con la información y los documentos cuando se extingue el contrato de servicios?

## 2.3. Almacenamiento *off-line* y *near-line*

Algunas organizaciones con grandes volúmenes de información electrónica se plantean en algunos casos el almacenamiento *off-line*, en el que la información se graba en dispositivos de almacenamiento. Ello ocurre cuando se quiere conservar la información, pero esta no va a ser utilizada con frecuencia. Actualmente, estas prácticas empiezan a ser menos comunes en las organizaciones, debido al abaratamiento de los costes de almacenamiento y al aumento de las capacidades.

Por ello el almacenamiento *off-line* y *near-line* está quedando relegado a las copias de seguridad. Aun así podemos encontrarlos en algunas organizaciones prácticas, como descargar documentos a CD o DVD para liberar espacio.

Cuando nos encontramos con este tipo de almacenamiento, debemos analizar cuáles son las decisiones que se han tomado al respecto y si su utilización responde a una práctica planificada o a una solución improvisada para solventar un problema puntual de almacenamiento. Desgraciadamente, en muchas organizaciones es frecuente encontrar información almacenada en soportes

*off-line*, desde cintas magnéticas a DVD o similares, que se realizaron en un momento determinado y que se siguen almacenando ya inservibles para la recuperación de la información.

El almacenamiento *near-line* es un tipo de almacenamiento intermedio entre el almacenamiento *on-line* y el *off-line*. En algunos casos la denominación *almacenamiento near-line* puede utilizarse para un determinado tipo de disco con altas capacidades de almacenamiento y velocidad de acceso lenta.

El sistema de almacenamiento *near-line* conoce en qué volumen residen los datos y usualmente puede "preguntar" a un robot para que lo pueda extraer de su localización física (una librería de cintas o un *jukebox* de discos) y colocarlo en el dispositivo de lectura, cuando desde una búsqueda *on-line* se requieren los datos contenidos en el repositorio *near-line*. Lógicamente la recuperación es más lenta que en un sistema *on-line*.

***Jukebox* óptico**

Un *jukebox* óptico es un dispositivo robótico que puede cargar y descargar discos ópticos, como CD, DVD o Blue-Ray. Puede tener más de 2.000 *slots* para discos y tiene un brazo que actúa sobre los discos y los *slots*. La organización de los discos y *slots* afecta al rendimiento del mismo, dependiendo de la cercanía entre discos y *slots*.

Este tipo de almacenamiento se produce habitualmente en organizaciones que tienen grandes volúmenes de información valiosa que ocupa mucho espacio. Un ejemplo claro son las organizaciones que manejan grandes cantidades de imágenes, como el centro de documentación de una televisión.

## 2.4. El caso especial del correo electrónico

La tecnología del correo electrónico ha creado en pocos años una forma muy diferente de comunicarse y la creación de un nuevo tipo de documentos electrónicos. Por la misma razón, la conservación y mantenimiento de los correos electrónicos se ha convertido en otro de los temas a solucionar. Dependiendo de las organizaciones podemos encontrar distintas estrategias que pueden variar, entre las cuales destacamos las siguientes:

- Imprimir copias en papel de los correos electrónicos, si bien la autenticidad y fiabilidad de estas copias es prácticamente nula.

- Sin intervención del usuario duplicar todos los mensajes trasmitidos a otro almacenamiento fuera del servidor, lo que fundamentalmente se hace cuando la organización se quiere curar en salud de los riegos de destrucción de e-mail.

- Establecer una serie de carpetas compartidas en el servidor, que permiten, ya sea de forma manual o automatizada, clasificar los correos en un estructura previamente establecida.

- Trasladar los correos electrónicos al repositorio documental corporativo mediante herramientas de usuario o sistemas automatizados. Esto normalmente conlleva la conversión de los correos electrónicos a otros formatos como PDF o XML.

Diferentes estudios realizados sobre el correo electrónico defienden que solo puede considerarse documentos a conservar un 10% de lo habitualmente recibido en un buzón. Sin embargo, pocas organizaciones han conseguido hacerlo eficazmente.

**Lectura recomendada**

Aunque visto desde la óptica de la preservación de los correos electrónicos, el siguiente documento es una excelente recopilación del estado del arte en la gestión de los correos electrónicos.

**Christopher Prom**. Preserving e-mail. Digital Preservation Coalition Technology Watch Report 11-01 December 2011.

La preocupación por la conservación de los correos electrónicos ha llevado al mercado de las tecnologías de la información a la comercialización de una tecnología específica que se conoce con la etiqueta de ***e-mail archiving***.

El *e-mail archiving* se define como el proceso de capturar, preservar y hacer fácilmente buscables todo el tráfico de correos electrónicos desde un individuo concreto, una organización o una unidad administrativa. Las soluciones de este tipo capturan el contenido de los correos, bien directamente sobre la aplicación de correo electrónico o en el proceso de comunicación, guardándolos en un almacenamiento que facilite su indexación y por lo tanto, su búsqueda.

Con este tipo de soluciones los departamentos de sistemas pueden al mismo tiempo descargar los servidores de correo y protegerse guardando todo el correo recibido. Esta segunda parte se ha potenciado mucho desde los entornos anglosajones y los departamentos legales que consideran que el correo es una fuente de *legal discovery* o soporte de pruebas en caso de litigio.

Para analizar el entorno de mantenimiento y conservación de los documentos, es muy importante saber si la organización ha implantado o va a implantar alguna solución de este tipo.

**Elección de una herramienta de *e-mail archiving***

Es interesante ver desde la perspectiva de las tecnologías de la información la manera de plantear, en una revista especializada, cómo elegir una herramienta de *e-mail archiving* en al año 2009.

http://www.eweek.com/c/a/Data-Storage/How-to-Choose-an-Email-Archiving-Solution/

# 3. Las políticas de conservación de la información electrónica

Habitualmente, en las organizaciones es responsabilidad de los servicios de informática el mantenimiento y conservación de los documentos y la información electrónica.

En el mundo de la tecnología 4 o 5 años es un tiempo larguísimo, durante el cual se puede haber cambiado toda la configuración informática más de una vez. Por tanto, en el plano tecnológico los conceptos de conservación a largo plazo tienen un significado mucho más corto de lo que se necesita para determinados documentos o información.

Cuando se realiza el análisis del entorno de conservación de los documentos electrónicos y las políticas que se pueden haber implementado desde los servicios de informática, debemos tener en cuenta esta diferencia de apreciación en los plazos.

En muchas organizaciones el crecimiento exponencial de la información electrónica almacenada es un verdadero problema para los servicios de informática. Si bien el tema económico no es el principal problema por el abaratamiento de los costes, sí lo es la complejidad de la gestión de una información que crece sin límites tendiendo al infinito. Por eso, en algunas organizaciones se fuerza el control poniendo límite a los espacios de almacenamiento o estableciendo bienintencionadas políticas de eliminación de la información, en base a periodos temporales establecidos de forma generalizada y arbitraria para toda la organización. En España es común la creencia de que los documentos solo deben guardarse 5 años. Este equívoco proviene de una mala interpretación tanto del Código de Comercio, como de la legislación fiscal. En el primer caso, el Código de Comercio dice que los empresarios deben guardar soporte documental de todos los asientos contables 6 años (la sabiduría popular los ha convertido en 5) después de haber presentado los libros contables. En el segundo caso, la legislación fiscal dice que los delitos fiscales prescriben a los 5 años.

Por otro lado, cuando se ha evitado eliminar información, es muy probable que la información electrónica con más de 5 o 6 años de antigüedad se haya guardado en formatos obsoletos, y es difícil consultarla y utilizarla. La obsolescencia de la información electrónica y su preservación a lo largo del tiempo es una de las preocupaciones universales en la que existen muy distintos enfoques y puntos de vista.

En todas las organizaciones que existen desde hace más de una década seguro que se han producido cambios de sistemas, actualizaciones de software, cambio de servidores o incluso cambio de sistemas operativos. Analizar si en estos

cambios se han producido pérdidas importantes de información o cómo se han abordado las migraciones y cambios de sistemas es una forma indirecta de averiguar cuáles son las políticas de conservación de la información electrónica, que en la mayor parte de los casos no habrán sido explicitadas como tales.

Sin embargo, también es posible que en determinadas organizaciones se haya reflexionado sobre el tema y se hayan establecido algunas medidas para la preservación de la información electrónica, e incluso planes de trasformación de la misma.

# 4. Las políticas de seguridad de la información

El incremento de recursos tecnológicos, la tendencia a trabajar cada vez más con recursos electrónicos, junto a la vulnerabilidad manifiesta en el acceso a información sensible –como ha quedado de manifiesto en acciones llevadas a cabo por parte de piratas informáticos– constituyen razones para que la seguridad de la información sea un aspecto clave en la gestión y preservación de documentos electrónicos de cualquier organización para poder continuar con su actividad diaria sin interrupciones.

Los documentos electrónicos deben ser objeto de las políticas de seguridad a fin de poder preservar las características de los documentos que dichas organizaciones originan.

Por ello dedicamos un módulo específico a la seguridad de la información. En primer lugar presentamos un breve esbozo del valor de las políticas de seguridad, y los esfuerzos que se están realizando desde distintas organizaciones. En segundo lugar presentamos los aspectos más relevantes que cualquier organización debe tener en cuenta en la definición de sus políticas de seguridad. Para ello nos basamos en los controles que define la norma ISO 27001, relacionados con la gestión de documentos.

## 4.1. El contexto y características de la información y los documentos

Durante la primera década del siglo XXI la seguridad de la información se ha desarrollado como un dominio específico y separado, que tiene sus propias normas y que ha arraigado en muchas organizaciones. La familia ISO 27000, Sistemas de gestión de la seguridad de la información, es el máximo exponente.

Desde los departamentos de tecnologías de la información se han ido desarrollando políticas, que aplican a toda la información electrónica que se guarda principalmente en los ordenadores, aunque en muchos discursos sobre el tema se hable de la información en general, que podría no necesariamente contenerse en los sistemas informáticos.

El enfoque de dichas políticas es fundamentalmente de protección de la información, estableciendo las medidas necesarias para evitar acceder a ella de forma no autorizada y que sea utilizada de forma maliciosa. De hecho, en el mundo de los piratas informáticos o *hackers*, del *spam* o del robo de identidades digitales, también se insiste mucho en la protección de los datos de carác-

ter personal y de la necesidad de crear confianza para el uso de los sistemas informáticos. Asimismo, muchas jurisdicciones establecen la obligatoriedad en el sector público de alguna forma de sistema de seguridad de la información.

**Real Decreto 1720/2007**

Ya en España en el derogado Real Decreto 994/1999, se aprobaban medidas de seguridad de los ficheros automatizados que contuviesen datos de carácter personal.

La misma voluntad de proteger los datos personales, más concretamente, "las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal", queda recogida en el actual Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Así pues, la seguridad de la información incluye tres dimensiones principales: la confidencialidad, la disponibilidad y la integridad de la información. Estos conceptos están recogidos en diferentes glosarios y aclaraciones terminológicas incluidas en documentos sobre seguridad de información. Aquí presentamos las expresadas en el documento ISO/IEC 13335-1:2004. La confidencialidad se refiere a que solo pueden acceder a la información aquellas personas que tienen autorización. Por disponibilidad entendemos el acceso a la información por parte de las personas autorizadas en el momento en que lo precisen. Por último, la integridad comprende la exactitud y completitud de los activos.

**Lectura recomendada**

ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

La integridad y la disponibilidad también son algunas de las características inherentes a los documentos –electrónicos o en papel–, junto a la autenticidad y fiabilidad. Su preservación permite que los documentos que genera la organización puedan actuar como evidencias de las actividades organizativas, y así posibilitar a las organizaciones la rendición de cuentas, como queda recogido en la norma ISO 15489. Esta norma define estas características de la siguiente manera:

La **autenticidad** de un documento se refiere a que este puede probar que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma. A tal fin, las organizaciones deben implantar y documentar políticas y procedimientos para controlar la creación, recepción, transmisión, mantenimiento y disposición de los documentos, de manera que se asegure que los creadores de dichos documentos estén autorizados e identificados, y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.

La **fiabilidad** es la característica que asegura que el contenido de dicho documento es una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio.

La **integridad** de un documento, como hemos apuntado antes, se refiere a que su contenido es completo y está inalterado. Para ello los documentos deben estar protegidos contra modificaciones no autorizadas. En caso de querer permitir adiciones o anotaciones, estas deben hacerse de acuerdo a políticas

y procedimientos de gestión que autoricen dichas adiciones o anotaciones. En el procedimiento se debe recoger qué adiciones o anotaciones se pueden realizar y a quién está permitido hacerlo. Asimismo, se debe dejar trazabilidad de los cambios: qué y quién los ha hecho.

La **disponibilidad** de un documento es la característica que permite localizarlo, recuperarlo, presentarlo e interpretarlo. Su presentación debería mostrar la actividad u operación que lo produjo, y mantener los vínculos entre los documentos que reflejan una secuencia de actividades, manteniéndose así el contexto de las actividades y las funciones de la organización.

**Lecturas recomendadas**

**UNE-ISO 15489-1:2006** Información y documentación. Gestión de documentos. Parte 1: Generalidades.

**UNE-ISO/TR 15489-2:2006** Información y documentación. Gestión de documentos. Parte 2: Directrices. (ISO/TR 15489-2:2001).

Teniendo en cuenta este contexto, y con el objetivo de asegurar la sostenibilidad de las organizaciones y minimizar los riesgos, desde distintos ámbitos se han propuesto una serie de medidas que cubren un amplio espectro de posibles amenazas sobre la información agrupadas en políticas, procedimientos, estructuras organizativas, software y hardware. A nivel organizativo, estas medidas quedan recogidas en las denominadas políticas de seguridad de la información.

En España, esta preocupación se ha materializado en el Esquema Nacional de Seguridad que se define en el Real Decreto 3/2010 de 8 de enero que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica. El ENS establece:

- los principios básicos,
- los requisitos mínimos,
- las medidas de seguridad que deben adoptarse,
- las comunicaciones electrónicas,
- la respuesta ante incidentes de seguridad,
- la certificación de seguridad,
- la conformidad.

En Europa, muchos países están utilizando la norma alemana de seguridad de tecnologías de la información desarrollada por la Oficina Federal para la Seguridad de la Información (Bundesamt für Sicherheit in der Informationstechnik, BSI). Su *Manual para la Protección* (IT-Grundschutz Handbuch, 2008) ha sido traducido a varias lenguas y su última versión incluye instrucciones para el análisis de riesgos que incluyen temas muy relacionados con la gestión de documentos, como los que provienen de la gestión del correo electrónico, de los sistemas de gestión de documentos, de las salvaguardias de datos, de los soportes de archivo, del intercambio de datos, y de los dispositivos móviles.

**Web recomendadas**

Bundesamt für Sicherheit in der Informationstechnik

Federal Office for Information Security

## 4.2. Los controles de la ISO 27001 y su relación con la gestión de documentos

Los controles de la ISO 27001 se refieren a la seguridad de la información. Intervienen cuando la información ya ha sido creada y almacenada y se encuentra en los ordenadores.

Los grados de seguridad son diversos. El máximo grado de seguridad sería el que sitúa la información en un bunker inaccesible. Todos sabemos que no se trata de eso, sino de encontrar el equilibrio entre las prácticas de seguridad necesarias para preservar la confidencialidad, disponibilidad e integridad de la información, y el uso de esta en las organizaciones.

La seguridad de la información tiene mucha relación con la gestión de los documentos electrónicos, si bien no todos los controles propuestos por la norma ISO 27001 están relacionados con la gestión de documentos o deben ser complementados en su visión para tener el alcance adecuado.

En consecuencia, cuando analizamos el contexto en el cual se mantienen y conservan los documentos electrónicos en las organizaciones que han implementado los controles de la ISO 27001, es frecuente que nos podamos encontrar con el discurso de que estos controles son más que suficientes para una adecuada gestión de los documentos electrónicos. A pesar de ello, hemos de analizar bien las arquitecturas y los sistemas de información, los lugares y las formas de almacenamiento, y las políticas definidas, para ver si los grados que se han definido son los adecuados para la preservación de documentos electrónicos.

La norma ISO 27001 ofrece pautas para identificar aspectos clave de un sistema de información. A fin de poder integrar en estas claves los aspectos de la gestión documental a tener en cuenta, a continuación presentamos las tablas que identifican los controles de la ISO 27001 relacionándolos con la gestión de los documentos electrónicos.

### 1) Política de seguridad

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.5.Política de seguridad | | | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.5.1.1 | Documento de política de seguridad de la información | La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados | Aunque algunos temas pueden ser coincidentes en la política de gestión documental y de seguridad de la información, el alcance y enfoque no es el mismo. El documento de política de seguridad de la información podría fusionarse con el documento de política de gestión de los documentos. |
| A.5.1.2 | Revisión de la política de seguridad | La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia | |

## 2) Aspectos organizativos

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.6. Aspectos organizativos | | | |
| A.6.1.1 | Compromiso de la Dirección con la seguridad de la información | La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y reconocimiento de las responsabilidades de seguridad d de la información | El mismo compromiso debería exigirse para la gestión de documentos |
| A.6.1.2 | Coordinación de la seguridad de la información | Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo | La coordinación en gestión de documentos también es necesaria |
| A.6.1.3 | Asignación de responsabilidades relativas a la seguridad | Deben definirse claramente todas las responsabilidades relativas a la seguridad | Las responsabilidades son otras |
| A.6.1.4 | Proceso de autorización de recursos para el tratamiento de la información | Para cada nuevo recurso de tratamiento de la información debe definirse e implantarse un proceso de autorización por parte de la dirección | En este mismo proceso de autorización debería incluirse la decisión de si con ese recurso se van a crear o no documentos. |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.6.1.5 | Acuerdos de confidencialidad | Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación que reflejen las necesidades de la organización para la protección de la información | Estos acuerdos de confidencialidad son aplicables a los documentos y a la información que contienen |
| A.6.1.6 | Contacto con las autoridades | Deben mantenerse los contactos adecuados con las autoridades pertinentes | Existen también autoridades en la gestión de los documentos |
| A.6.1.7 | Contacto con grupos de especial interés | Deben mantenerse los contactos adecuados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad | Existen también grupos de interés especializados en gestión de documentos |
| A.6.1.8 | Revisión independiente de la seguridad de la información | El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad | Esta revisión independiente también puede hacerse de la gestión de documentos. |
| A.6.2.1 | Identificación de los riesgos derivados del acceso de terceros | Deben identificarse los riesgos para la información y los dispositivos de tratamiento de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso | Estos controles son aplicables en los caos en que terceros o clientes deban acceder a los documentos de la organización, y especialmente cuando se externalice algún proceso de negocio o la propia gestión de los documentos |
| A.6.2.2. | Tratamiento de la seguridad en relación con los clientes | Deben tratarse todos los requisitos de seguridad identificados antes de otorgar acceso a los clientes a los activos o información de la organización | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.6.2.3. | Tratamiento de la seguridad en contratos con terceros | Los acuerdos con terceros que conlleven acceso, procesado, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien de la incorporación de productos y servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos pertinentes | |

### 3) Gestión de activos

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.7. Gestión de activos | | | |
| A.7.1.1. | Inventario de activos | Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes | Los documentos son un activo de la información y por lo tanto deberían incluirse en este inventario, si bien desde gestión documental se propone que además exista una identificación previa de los documentos que deben crearse en cada proceso de negocio |
| A.7.1.2 | Propiedad de los activos | Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como tal | El concepto de propietario o responsable de aplicaciones informáticas puede encajar si determinamos que por ejemplo un EDMRS es propiedad de la Unidad de gestión documental. Sin embargo si descendemos a los propios documentos desde gestión documental se insiste en que los documentos de una organización son un activo corporativo |
| A.7.1.3. | Uso aceptable de los activos | Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el tratamiento de la información | Este control puede ser aplicable a los documentos |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.7.2.1 | Directrices de clasificación | La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización | La clasificación de seguridad y los posibles metadatos que genera son sólo un aspecto de la clasificación y metadatos que se requieren para los documentos |
| A.7.2.2. | Etiquetado y manipulado de la información | Se debe desarrollar e implantar un con junto adecuado de procedimientos para etiquetar y manejar información de acuerdo con el esquema de clasificación adoptado por la organización | |

## 4) Recursos humanos

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.8 Recursos humanos | | | |
| A.8.1.1 | Funciones y responsabilidades | Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros de deben definir y documentar de acuerdo con la política de seguridad de la información de la organización | Las medidas con respecto a los recursos humanos antes de la contratación son válidas enfocándolo a la gestión de los documentos |
| A.8.1.2. | Investigación de antecedentes | La comprobación de antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.8.1.3 | Términos y condiciones de contratación | Como parte de sus obligaciones contractuales los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en los relativo a seguridad de la información | |
| A.8.2.1 | Responsabilidades de la Dirección | La Dirección debe exigir a los empleados, contratistas y terceros que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización | Lo mismo debe suceder con las políticas y procedimientos de la gestión documental |
| A.8.2.2 | Concienciación, formación y capacitación en seguridad de la información | Todos los empleados de la organización, y cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo | También debe existir una concienciación y capacitación en la gestión de los documentos |
| A.8.2.3 | Proceso disciplinario | Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad | Este control sería aplicable a la gestión de los documentos |
| A.8.3.1 | Responsabilidad de cese o cambio | Las responsabilidades para proceder al cese en el empleo o cambio de puesto de trabajo deben estar claramente definidas y asignadas | Los controles al finalizar la relación de un trabajador con la organización son aplicables también en el caso de los documentos |
| A.8.3.2 | Devolución de activos | Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.8.3.3. | Retirada de los derechos de acceso | Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos | |

## 5) Seguridad física y ambiental

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.9 Seguridad física y ambiental | | | |
| A.9.1.1 | Perímetro de seguridad física | Se deben utilizar perímetros de seguridad (barreras, muros puerta de entrada con control de acceso a través de tarjeta, o puesto de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información | Todos los controles de seguridad física y ambiental son aplicables tanto a los ordenadores y sistemas informáticos donde se gestionan los documentos electrónicos, como a los espacios e instalaciones donde se custodian documentos en papel |
| A.9.1.2 | Controles físicos de entrada | Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado | |
| A.9.1.3 | Seguridad de oficinas, despachos e instalaciones | Se deben diseñar y aplicar medidas de seguridad física para las oficinas, despachos e instalaciones | |
| A.9.1.4 | Protección contra las amenazas externas de origen ambiental | Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otra forma de desastres naturales o provocados por el hombre | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.9.1.5 | Trabajo en áreas seguras | Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en áreas seguras | |
| A.9.1.6 | Áreas de acceso público y carga y descarga | Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de las instalaciones de tratamiento de la información para evitar accesos no autorizados | |
| A.9.2.1 | Emplazamiento y protección de equipos | Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados | |
| A.9.2.2. | Instalaciones de suministro | Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro | |
| A.9.2.3. | Seguridad de cableado | El cableado eléctrico y de telecomunicaciones que trasmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones | |
| A.9.2.4 | Mantenimiento de equipos | Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad e integridad | |
| A.9.2.5 | Seguridad de los equipos fuera de las instalaciones | Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera de las instalaciones | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.9.2.6 | Reutilización o retirada segura de equipos | Todos los soportes de almacenamiento deben ser comprobados para confirmar que todos los datos sensibles y todas las licencias de software se han eliminado o bien se han borrado o sobreescrito de manera segura, antes de su retirada | |
| A.9.2.7 | Retirada de materiales propiedad de la empresa | Los equipos, la información o el software no deben sacarse de las instalaciones sin una autorización previa | |

## 6) Gestión de comunicaciones y operaciones

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.10. Gestión de comunicaciones y operaciones | | | |
| A.10.1.1. | Documentación de los procedimientos de operación | Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten | También deben existir procedimientos de operación de gestión de documentos electrónicos |
| A.10.1.2 | Gestión de cambios | Deben gestionarse los cambios en los sistemas de tratamiento de la información | Aplicable a los sistemas que gestionan documentos electrónicos |
| A.10.1.3 | Segregación de tareas | Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización | Este control es difícilmente aplicable a la tareas y responsabilidades de gestión documental |
| A.10.1.4 | Separación de los recursos de desarrollo, prueba y operación | Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema de producción | Aplicable en los sistemas informáticos que gestionan documentos electrónicos |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.10.2.1 | Provisión de servicios | Se deben comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero | Estos controles serían aplicables a los documentos cuando se han encargado a un tercero tareas que crean y gestionan documentos o la propia gestión de los mismos |
| A.10.2.2. | Supervisión y revisión de los servicios prestados por terceros | Los servicios, informes y registros proporcionados por un terceros deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorías periódicas | |
| A.10.2.3 | Gestión del cambio en los servicios prestados por terceros | Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riegos | |
| A.10.3.1 | Gestión de capacidades | La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema | Estos controles son aplicables para los sistemas que gestionan documentos electrónicos |
| A.10.3.2 | Aceptación del sistema | Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente aceptación | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| 10.4.1 | Controles contra el código malicioso | Se deben implantar controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario | Estos controles son aplicables para los sistemas que gestionan documentos electrónicos |
| A.10.4.2 | Controles contra el código descargado en el cliente | Cuando se autorice el uso de código descargado en el cliente, la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute un código no autorizado | |
| A.10.5.1 | Copias de seguridad de la información | Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente conforme a la política de copias de seguridad acordada | Este control es aplicable a los sistemas que gestionan documentos electrónicos pero en ningún caso sustituyen a la implantación de procesos de evaluación, disposición y preservación de los documentos electrónicos |
| A.10.6.1 | Controles de red | Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo información en tránsito | Estos controles son aplicables cuando los sistemas informáticos que gestionan documentos electrónicos se instalan en red |
| A.10.6.2. | Seguridad de servicios de red | Se deben identificar las características de seguridad, los niveles de servicio de red, tanto si estos servicios se prestan dentro de la organización o se subcontratan | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.10.7.1 | Gestión de soportes extraíbles | Se deben establecer procedimientos para la gestión de soportes extraíbles | Estos controles son aplicables para los soportes extraíbles que permitan los sistemas informáticos que gestionan documentos electrónicos |
| A.10.7.2 | Retirada de soportes | Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos | |
| A.10.7.3 | Procedimientos de manipulación de la información | Deben establecerse los procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o uso indebido | Deben existir procedimientos específicos para la manipulación y gestión de documentos |
| A.10.7.4 | Seguridad de la documentación del sistema | La documentación del sistema debe estar protegida contra accesos no autorizados | La documentación de los sistemas debe incluirse en la política general de gestión de documentos |
| A.10.8.1 | Políticas y procedimientos de intercambio de información | Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación | Deben existir procedimientos específicos para la manipulación y gestión de documentos |
| A.10.8.2 | Acuerdos de intercambio | Deben establecerse acuerdos para el intercambio de información y de software entre la organización y terceros | Estos controles son aplicables a los sistemas informáticos que crean y gestionan documentos electrónicos |
| A.10.8.3 | Soportes físicos en tránsito | Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro | |
| A.10.8.4 | Mensajería electrónica | La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.10.8.5 | Sistemas de información empresariales | Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales | |
| A.10.9.1 | Comercio electrónico | La información incluida en el comercio electrónico que se trasmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información | Estos controles son aplicables para los sistemas informáticos que crean y gestionan documentos electrónicos y cuya operación incluye comercio electrónicos, transacciones en línea o información pública |
| A.10.9.2 | Transacciones en línea | La información contendida en las transacciones en línea debe estar protegida para evitar trasmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizada del mensaje | |
| A.10.9.3 | Información públicamente disponible | La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas | |
| A.10.10.1 | Registro (log)de auditorías | Se deben generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberían mantener estos registros durante un período de tiempo acordado para servir como prueba en investigaciones futuras y en la supervisión de control de acceso | Estos controles son aplicables para los sistemas informáticos que crean y gestionan documentos electrónicos |
| A.10.10.2 | Supervisión de uso del sistema | Se deben establecer procedimientos para supervisar el uso de los recursos de tratamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.10.10.3 | Protección de la información de los registros (logs) | Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados | |
| A.10.10.4 | Registros (log) de administración y operación | Se deben registrar las actividades del administrador del sistema y de la operación del sistema | |
| A.10.10.5 | Registro (log) de fallos | Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones | |
| A.10.10.6 | Sincronización de reloj | Los relojes de todos los sistemas de tratamiento de la información dentro de una misma organización o un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada en el tiempo | |

## 7) Control de acceso

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.11 Control de acceso | | | |
| A.11.1.1 | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso | La política de acceso a los documentos debe estar definida de la misma forma. Supone una profundización en el control propuesto |
| A.11.2.1 | Registro de usuario | Debe establecerse un procedimiento formal de registro y anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos y son coincidentes con los propuestos desde gestión documental |
| A.11.2.2 | Gestión de privilegios | La asignación y el uso de privilegios deben estar restringidos y controlados | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.11.2.3 | Gestión de contraseñas de usuarios | La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal | |
| A.11.2.4. | Revisión de los derechos de acceso de usuario | La dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal | |
| A.11.3.1 | Uso de contraseñas | Se debe requerir a los usuarios seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos |
| A.11.3.2. | Equipo de usuario desatendido | Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada | |
| A.11.3.3. | Política de trabajo despejado y pantalla limpia | Debe adoptarse una política de puesto de trabajo despejado de papeles y soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de tratamiento de la información | |
| A.11.4.1 | Política de uso de los servicios en red | Se debe proporcionar a los usuarios únicamente el acceso a los servicios para los que hayan sido específicamente autorizados | Estos controles actúan en una capa previa a la de los sistemas informáticos que crean y gestionan documentos |
| A.11.4.2. | Autenticación de usuario para conexiones externas | Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos | |
| A.11.4.3 | Identificación de los equipos en las redes | La identificación automática de los equipos de debe considerar un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos | |
| A.11.4.4. | Diagnóstico remoto y protección de los puertos de configuración | Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.11.4.5 | Segregación de redes | Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes | |
| A.11.4.6 | Control de la conexión a la red | En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales | |
| A.11.4.7 | Control de encaminamiento (*routing*) de red | Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso a las aplicaciones empresariales | |
| A.11.5.1 | Procedimientos seguros de inicio de sesión | El control a los sistemas operativos de debe controlar por medio de un procedimiento seguro de inicio de sesión | Estos controles actúan en una capa previa a la de los sistemas informáticos que crean y gestionan documentos |
| A.11.5.2 | Identificación y autenticación de usuario | Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada al usuario | |
| A.11.5.3 | Sistema de gestión de contraseñas | Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas de calidad | |
| A.11.5.4. | Uso de los recursos del sistema | Se debe restringir y controlar de una manera rigurosa el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de aplicación | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.11.5.5. | Desconexión automática de sesión | Las sesiones inactivas deben cerrarse después de un período de inactividad definido | |
| A.11.5.6 | Limitación del tiempo de conexión | Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión | |
| A.11.6.1 | Restricción de acceso a la información | Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida | El acceso a los documentos se define en las tablas de seguridad y acceso. Sería un detalle del acceso a la información |
| A. 11.6.2 | Aislamiento de sistemas sensibles | Los sistemas sensibles deben tener un entorno dedicado (aislado) de ordenadores | Este control puede ser aplicable a los entornos donde se guardan los documentos vitales o esenciales de una organización |
| A.11.7.1 | Ordenadores portátiles y comunicaciones móviles | Se deben implantar una política formal y se deben adoptar las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles | Estos controles aplican a la gestión de documentos mediante dispositivos portátiles o móviles y el acceso a los sistemas que gestionan documentos mediante teletrabajo. |
| A.11.7.2 | Teletrabajo | Se deben redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes | |

## 8) Adquisición, desarrollo y mantenimiento de los sistemas de información

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información | | | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.12.1.1 | Análisis y especificación de los requisitos de seguridad | En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad | También deberían incluirse los requisitos de la gestión de documentos en los sistemas de información que los creen o los gestionen |
| A.12.2.1 | Validación de datos de entrada | La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos |
| A.12.2.2 | Control de procesamiento interno | Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones | |
| A.12.2.3 | Integridad en los mensajes | Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados | |
| A.12.2.4 | Validación de los datos de salida | Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias | |
| A.12.3.1 | Política de usos de los controles criptográficos | Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información | Estos controles son especialmente significativos en la gestión de documentos y especialmente cuando se utilizan firmas digitales |
| A.12.3.2 | Gestión de claves | Debe implantarse un sistema de gestión de claves para dar soporte al uso de las técnicas criptográficas por parte de la organización | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.12.4.1 | Control del software en explotación | Deben estar implantados procedimientos para controlar la instalación de software en los sistemas en producción o en explotación | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos |
| A.12.4.2 | Protección de los datos de prueba del sistema | Los datos de prueba se deben seleccionar cuidadosamente y deben estar protegidos y controlados | |
| A.12.4.3 | Control de acceso al código fuente de los programas | Se debe restringir el acceso al código fuente de los programas | |
| A.12.5.1 | Procedimientos de control de cambio | La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos |
| A.12.5.2 | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización | |
| A.12.5.3 | Restricciones a los cambios en los paquetes de software | Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso | |
| A.12.5.4 | Fugas de información | Deben evitarse las situaciones que permitan que se produzcan fugas de información | |
| A.12.5.5 | Externalización del desarrollo de software | La externalización del desarrollo de software debe ser supervisada y controlada por la organización | |
| A.12.6.1 | Control de la vulnerabilidades técnicas | Se debe obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización | Estos controles son aplicables a los sistemas informáticos que gestionan documentos electrónicos |

## 9) Gestión de incidentes de seguridad

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.13 Gestión de incidentes de seguridad | | | |
| A.13.1.1. | Notificación de eventos de seguridad de la información | Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible | Estos controles son aplicables para incidentes de seguridad que puedan producirse en el estén implicados documentos de la organización |
| A.13.1.2 | Notificación de los puntos débiles de seguridad | Todos los empleados, contratistas y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios | |
| A.13.2.1 | Responsabilidades y procedimientos | Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información | |
| A.13.2.2. | Aprendizaje de los incidentes de seguridad de la información | Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información | |
| A.13.2.3. | Recopilación de evidencias | Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, y conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente | |

## 10) Gestión de la continuidad del negocio

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.14 Gestión de la continuidad del negocio | | | |
| A.14.1.1 | Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio | Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio | La continuidad del negocio es uno de los puntos que están más relacionados con la gestión documental. En los procesos documentales siempre se incluye la identificación de los documentos vitales y esenciales que deben gestionarse de forma que aseguren la continuidad del negocio |
| A.14.1.2 | Continuidad del negocio y evaluación de riesgos | Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como las probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información | |
| A.14.1.3 | Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información | Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos críticos de negocio | |
| A.14.1.4 | Marco de referencia para la planificación de la continuidad del negocio | Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y del mantenimiento | |
| A.14.1.5 | Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio | Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos | |

## 11) Cumplimientos

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.15 Cumplimiento | | | |
| A.15.1.1 | Identificación de la legislación aplicable | Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícita para cada sistema de información de la organización | Este es un punto clave en la gestión de documentos, que amplía el alcance de la legislación a tener en cuenta |
| A.15.1.2 | Derechos de propiedad intelectual | Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual pueden existir derechos de propiedad intelectual y sobre uso de productos de software propietario | En determinados entornos la gestión de los documentos debe aclarar este punto |
| A. 15.1.3 | Protección de los documentos de la organización | Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales | Este es el único control que se refiere específicamente a los documentos. En un solo control se abarcan todos los procesos y requisitos documentales |
| A.15.1.4 | Protección de datos y privacidad de la información de carácter personal | Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes | De especial aplicación en la gestión documental |
| A.15.1.5 | Prevención del uso indebido de los recursos de tratamiento de la información | Se debe disuadir a los usuarios de utilizar los recursos de tratamiento de la información para fines no autorizados | |
| A.15.1.6 | Regulación de los controles criptográficos | Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes. | |

| Controles ISO 27001 | | | Relación con la gestión de documentos |
|---|---|---|---|
| **Código** | **Nombre** | **Control** | |
| A.15.2.1 | Cumplimiento de las políticas y normas de seguridad | Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad | Lo mismo debería suceder con los procedimientos de gestión documental |
| A.15.2.2 | Comprobación del cumplimiento técnico | Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación para la implantación de la seguridad | |
| A.15.3.1 | Controles de auditoría de los sistemas de información | Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas de producción deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos del negocio | Los mismos controles serian aplicables a las auditorías sobre los sistemas de información que crean o gestionan documentos electrónicos<br>También podrían existir controles propios referido a auditorías sobre los procesos y controles documentales |
| A.15.3.2 | Protección de las herramientas de auditoría de los sistemas de información | El acceso a las herramientas de auditoría de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido | |

# Bibliografía

**Barlett, M.** (2009). "How to Choose an E-mail Archiving Solution. eweek". Disponible en http://www.eweek.com/c/a/Data-Storage/How-to-Choose-an-Email-Archiving-Solution/ [Consulta: enero del 2013].

**Bundesamt für sicherheit in der informationstechnik** (2008). *IT-Grundschutz Handbuch, 2008*. Disponible en https://www.bsi.bund.de/DE/Home/home_node.html [Consulta: 15 de octubre del 2012].

**Cruz Allende, D.; Garre Gui, S.** (2011). *Sistema de gestión de la seguridad de la información*. Barcelona: Universitat Oberta de Catalunya.

**González Fernández, V. R.** Trabajo en colaboración apoyado en la red. Para la Inspección de Educación de Castilla y León http://platea.pntic.mec.es/vgonzale/trabcolab_0910/index.htm

**Graham, T.** (2003). "Electronic access to and the preservation of heritage materials". *The Electronic Library* (vol. 21, núm. 3, pág. 223-226).

**Groenewald, R.; Breytenbach, A.** (2011). "The use of metadata and preservation methods for continuous access to digital data". *The Electronic Library* (vol. 29, núm. 2, pág. 236-248).

ICT Policy and Coordination Office. Department of Public Works (2011). Information Standars 18: Information Security – Implementation Guideline. Queensland Government. Disponible en: http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/IS18%20-%20Implementation%20Guideline.pdf [Consulta: 15 de octubre de 2012]

ICT Policy and Coordination Office. Department of Public Works (2010). Email disclaimer guideline. Disponible en: http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGEA%202.0/Email%20disclaimer%20guideline.pdf [Consulta: 15 de octubre de 2012]

ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

**Krtalic, M.; Hasenay, D.** (2012). "Exploring a framework for comprehensive and successful preservation management in libraries". *Journal of Documentation* (vol. 68, núm 3, pág. 353-377).

**Lin, L. S.; Ramaiah, Ch. K.; Wal, P. K.** (2003). "Problems in the preservation of electronic Records". *Library Review* (vol. 52, núm. 3, pág. 117-125).

**Prom, Ch.** (2011). *Preserving e-mail*. Digital Preservation Coalition Technology Watch Report 11-01 December 2011. DOI.

UNE-ISO 15489-1:2006 Información y documentación. Gestión de documentos. Parte 1: Generalidades.

UNE-ISO/TR 15489-2:2006 Información y documentación. Gestión de documentos. Parte 2: Directrices. (ISO/TR 15489-2:2001).

**Zierau, Eld Maj-Britt Olmütz** (2012). "A holistic approach to bit preservation". *Library Hi Tech* (vol. 30, núm. 3, pág. 472-489).