G03/D02/G

Directrices – Seguridad de la información

Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de transparencia y Acceso a la Información (RTA)

Versión: 1.0

Fecha: diciembre de 2014

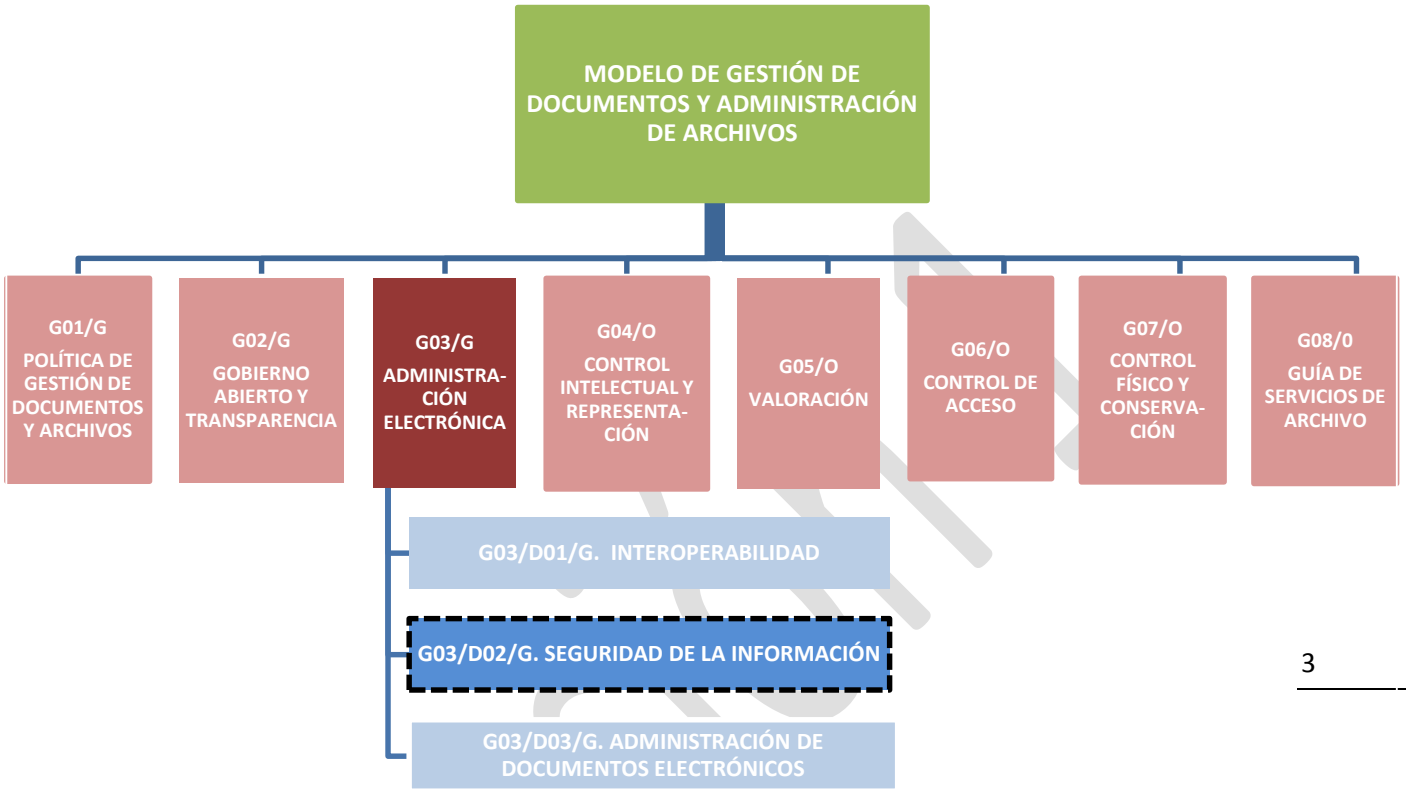
Coordinadores

Beatriz Franco Espiño
Ricard Pérez Alcázar

Equipo

Blanca Desantes Fernández
Francisco Fernández Cuesta
Javier Requejo Zalama

Estas Directrices se integran en el MGD según se especifica en el siguiente Diagrama de relaciones:



1. Presentación y objetivos

1.1. Finalidad

La finalidad de estas Directrices es proporcionar recomendaciones para la necesaria seguridad de la información en el ámbito de la administración electrónica, con respeto a la autonomía de las organizaciones y en el marco del Modelo de Gestión de Documentos y administración de archivos de la Red de Transparencia y Acceso a la información (RTA).

1.2. Alcance y contenido

Esta directriz sobre la Seguridad de la información se fundamenta en la norma ISO/IEC 27002:2013. *Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información*, que es una reconversión de la antigua norma ISO/IEC17799.

VILLALÓN HUERTA, A. 2004. *Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799*. Disponible en: http://www.shutdown.es/ISO17799.pdf

De este modo, tras una relación de los principios básicos que afectan a la seguridad de la información, las entradas del capítulo dedicado a la Política de seguridad respetarán en su estructura las cláusulas contempladas en la norme ISO/IEC27002:2013, a saber:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones

- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

1.3. Documentos relacionados

G03/G	Administración electrónica
G03/D01/G	Interoperabilidad
G03/D03/G	Administración de los documentos electrónicos

2. Concepto de seguridad de la información

Ante la imparable y necesaria interconexión, los sistemas y las redes de información presentan una mayor vulnerabilidad. Su exposición a una gran variedad de amenazas urge a la resolución de nuevos retos en el campo de la seguridad de la información. Se hace necesaria una mayor concienciación y comprensión de todos los aspectos relacionados con dicha seguridad, que se deben conformar como premisas para una cultura de la seguridad.

Junto a la interoperabilidad, la seguridad adquiere un rol crítico en el marco de una administración electrónica, al deber soportar derechos como el de la garantía de la seguridad y la confidencialidad de los datos contenidos en ficheros, sistemas y aplicaciones.

En el contexto de la administración electrónica, la seguridad de la información se define como aquella capacidad de las redes o de los sistemas de información para resistir, manteniendo un adecuado nivel de confianza, los accidentes o las acciones ilícitas o malintencionadas que comprometan la disponibilidad, la autenticidad, la integridad y la confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

3. Principios de la seguridad de la información

En un documento publicado en 2002, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) estimaba que los principios relativos a la seguridad se podían resumir en nueve apartados, que son los siguientes:

1. **Concienciación**. Hay que adquirir conciencia de la necesidad de disponer de sistemas y redes de información seguros, al tiempo que conocer los medios para ampliar la seguridad.
2. **Responsabilidad**. Todos los actores implicados en la gestión de los documentos electrónicos son responsables de la seguridad de la información.
3. **Respuesta**. Hay que desarrollar actuaciones conjuntas y pertinentes para prevenir, detectar y responder a los incidentes que afecten a la seguridad.

4. **Ética**. Hay que contemplar los intereses legítimos de terceros.
5. **Democracia**. Hay que compatibilizar la seguridad y los valores esenciales de una sociedad democrática.
6. **Evaluación del riesgo**. Hay que llevar a cabo evaluaciones de riesgo.
7. **Diseño y realización de la seguridad**. Hay que incorporar la seguridad como un elemento esencial de los sistemas y redes de la información.
8. **Gestión de la seguridad**. Hay que adoptar una visión integral de la seguridad en la administración electrónica.
9. **Reevaluación**. Hay que revisar y reevaluar la seguridad de la información y realizar aquellas modificaciones pertinentes sobre políticas, prácticas, medidas y procedimientos relativos a la seguridad.

4. Política integral de seguridad

La información que se gestiona mediante sistemas o redes, en el ámbito de la administración electrónica, básicamente se encuentra en tres estados: transmisión, almacenamiento y proceso. Con independencia de su estado, sea cual sea la forma que adquiera y los medios utilizados en cualquier situación, esa información debe protegerse de manera correcta.

La política de seguridad debe garantizar las siguientes características fundamentales de la información:

- **Confidencialidad**. Seguridad de prevención frente a la disposición, la comunicación y la divulgación de información a terceros no autorizados
- **Integridad**. Seguridad de prevención ante la transformación o la modificación no autorizada durante su tratamiento o el almacenamiento de la información, con la exigencia de una rápida observación de alteraciones
- **Disponibilidad**. Seguridad de facilitar el acceso a la información por parte de quien esté autorizado y seguridad de prevención contra denegaciones a accesos autorizados
- **Autenticidad**. Seguridad frente a la identidad del productor o emisor de la información
- **Conservación**. Seguridad frente al deterioro de la información, mediante medidas preventivas y de preservación durante todo el ciclo de vida de los documentos
- **Trazabilidad**. Seguridad frente al conocimiento de operaciones, consultas o modificaciones de la información.

4.1. Política de seguridad

Los equipos directivos de las organizaciones marcarán las directrices en materia de seguridad de la información, de modo que se alineen con los objetivos de sus propios servicios. Dichos equipos demostrarán su apoyo y su compromiso con la publicación y mantenimiento de una política de seguridad de la información en sus organizaciones, que deberá garantizar la confidencialidad, la integridad, la disponibilidad, la autenticidad, la conservación y la trazabilidad.

Esta voluntad política de la seguridad se materializará en un documento que recoja las disposiciones vigentes sobre la materia, los estándares y los procedimientos de las organizaciones, de modo que se defina un marco de aplicación. Este documento debe ser

aprobado al más alto nivel directivo y comunicado a toda la organización de modo comprensible. Los contenidos del documento pueden ser:

- Definición, objetivos y alcance
- Compromiso directivo
- Marco referencial, con objetivos de control y evaluación del riesgo
- Principios, estándares y requerimientos de la seguridad
- Definición de responsabilidades

La política de seguridad de la información de las organizaciones se actualizará periódicamente, en función de los cambios legislativos, del análisis de riesgos, de los cambios estructurales o como el fruto de la misma experiencia, en aras de su idoneidad, su eficiencia y su efectividad. Para ello se establecerán cronogramas o períodos de revisión.

4.2. Aspectos organizativos de la seguridad de la información

En el aspecto organizativo, se distinguirá entre la gestión de la seguridad de la información en el seno de la propia administración y la seguridad que se mantenga respecto de los activos de información que sean accesibles por usuarios externos u otras organizaciones.

En la primera de las situaciones, se parte de un documento formalmente aprobado y la posterior asignación de los roles de seguridad, así como la coordinación y revisión de la implementación en toda la organización.

- **Compromiso del equipo directivo con la seguridad**. La mejor declaración de compromiso es la asignación específica de roles, la asignación de los recursos necesarios y el inicio de planes de concienciación.
- **Coordinación de la seguridad**. La coordinación dentro de la organización requiere de participación de diferentes sectores, con roles y funciones relevantes.
- **Asignación de roles**. Es necesario que se definan las responsabilidades sobre la seguridad. Las tareas pueden delegarse, pero no eximirá de la responsabilidad.
- **Revisión independiente de la seguridad**. La revisión del enfoque sobre la gestión de la seguridad es necesario que se lleve a cabo por personal externo, para que se considere realmente independiente.

En la segunda, se debe controlar el acceso, el tratamiento y la comunicación de la información efectuados por externos. La seguridad de la información y de sus medios de tratamiento no debe reducirse ante la introducción de productos o servicios externos.

En este sentido, se considerará lo siguiente:

- **Identificación de los riesgos**. Para lo cual se deben introducir controles apropiados antes de permitir el acceso. Además, cabe la firma de un contrato en el que se definan los términos y condiciones para la conexión y el acceso.
- **Tratamiento de la seguridad**. Se tratarán los términos de seguridad antes de permitir cualquier acceso a los activos de la organización, que dependerán según los medios de tratamiento y la información a la que se dé acceso. Al igual que en el punto anterior, se considerará la oportunidad de gestionar las condiciones mediante la firma de acuerdos

que contemplen requerimientos específicos de seguridad sobre la tecnología y las actividades.

4.3. Seguridad ligada a los recursos humanos

En este punto, el objetivo principal es asegurar que cualquier persona que participe en la organización conozca y acepte la responsabilidad que conlleva la seguridad de la información, de sus sistemas y sus redes. Se cubrirá la confidencialidad con el recurso de cláusulas específicas, que refieran obligaciones y responsabilidades. De manera subsidiaria, se perseguirá la disminución de fraudes o acciones malintencionadas. (Véase la directriz *G01/D03/G. Roles, responsabilidades y competencias*).

El apartado de seguridad de la información respecto de los recursos humanos va ligado a la necesidad de formación del personal y el desarrollo de planes de concienciación. Un conocimiento de la importancia de la seguridad conllevará un mejor conocimiento de las propias responsabilidades y de las medidas de control.

En cuanto a la selección del personal, estas medidas se orientarán a:

- **Roles y responsabilidades**. Definición y comunicación documentada de los roles y las responsabilidades de la seguridad a todo posible empleado de la organización durante el proceso de selección de personal.
- **Términos y condiciones del empleo**. Inclusión de términos y condiciones de seguridad en el contenido de los contratos, donde se refieran las responsabilidades.

En cuanto al personal activo, estas medidas se orientarán a:

- **Responsabilidades del equipo directivo**. Requerirán a todo el personal (interno y externo) que apliquen por igual la seguridad, según la política procedimientos establecidos. Deben asegurarse de que el personal está apropiadamente informado de sus roles, las expectativas de seguridad, además de fomentar una concienciación que suponga una motivación añadida.
- **Capacitación en seguridad**. El personal de la organización debe ser capacitado en materia de seguridad de la información y sus conocimientos sobre políticas y procedimientos deben actualizarse. Esta capacitación incluirá los requerimientos de seguridad, las responsabilidades legales, el uso de los medios de tratamiento y la información de los posibles procesos disciplinarios consecuentes a una deficiente praxis. Esta capacitación será adecuada a los roles que desarrollen en la organización, porque el objetivo último es reconocer problemas y responder a las necesidades.

En cuanto al personal saliente, estas medidas se orientarán a:

- **Responsabilidades finales**. Definición de responsabilidades relacionadas tras el abandono del puesto en la organización, con recordatorio de las relativas a la seguridad y las legales, como pudieran ser acuerdos de confidencialidad.
- **Devolución de activos**. La terminación de un contrato laboral implicará la devolución de aquellos activos que el personal saliente pudiera tener en su posesión, bien software o documentos corporativos.

- **Retirada de derechos de acceso**. De igual manera, debieran retirarse todos los derechos de acceso tras la terminación de contrato laboral al personal saliente. Haber considerado documentalmente la relación entre el acceso y la vigencia del contrato, significará sólo el recordatorio del cumplimiento de la legalidad.

4.4. Seguridad física y ambiental

Este apartado se centra en la protección de los activos físicos a través del control de acceso y la protección contras posibles contingencias externas.

La infraestructura que sustentan las aplicaciones informáticas que soportan la tramitación, como también los soportes de almacenamiento, bien se hallen en la misma sede de la organización o bien externalizados, requieren de protección mediante un control de acceso físico que garantice un acceso del personal autorizado.

Para ello, la infraestructura se ubicará en áreas de acceso restringido mediante niveles de seguridad. Todo acceso se registrará por los mecanismos de control de acceso, como posible prueba ante auditorías. Pero los sistemas y la información soportada también deben protegerse ante amenazas físicas o ambientales.

Las áreas seguras son aquéllas donde se encuentran los medios de tratamiento de información crítica o confidencial y están protegidas por perímetros de seguridad, además de barreras y controles de entrada.

- **Perímetro de seguridad física**. Protegen las áreas que contienen información y medios de tratamiento de información. La protección física se conseguirá creando barreras físicas alrededor de los locales. Los perímetros tendrán, entre otras, las siguientes características: definición, solidez física, control físico de acceso, salidas de emergencia con alarma.
- **Controles de ingreso físico**. Permiso de ingreso sólo a personal autorizado, con control horario, limitaciones a salas con información sensible, uso de acreditaciones y actualización de permisos.
- **Seguridad de oficinas y medios**. Especial diseño de los lugares con especial control del acceso.
- **Protección contra amenazas externas e internas**. Protección contra daños motivados por el fuego, inundaciones, terremotos, explosiones, revueltas u otros desastres naturales o causados por el hombre.
- **Áreas de acceso público, entrega y carga.** Control de los puntos de acceso donde transiten personas externas a la organización, para evitar su acceso a zonas no autorizadas.

En cuanto a la seguridad del equipo, el objetivo es evitar sustracciones o pérdidas de los activos y actividades de la organización. La protección sopesará amenazas físicas y ambientales.

- **Ubicación y protección del equipo**. Reducción de amenazas, peligros ambientales y accesos no autorizados. Algunas acciones serán, entre otras, las siguientes: reducción

del acceso, monitoreo de las condiciones ambientales, especial protección de equipos con información confidencial.

- **Servicios públicos de soporte**. Protección ante posibles fallas o interrupciones de energía. Las rutinas de inspección y el desarrollo de planes de contingencia pueden minimizar sus riesgos.
- **Seguridad del cableado**. Protección ante su intercepción o daño. Se considera dedicarle una atención y protección especial, ante posibles hurtos, interferencias o manipulación no autorizada.
- **Mantenimiento de equipos**. Garantizar su integridad y continua disponibilidad. Cabrá seguir las indicaciones del proveedor, ordenar las reparaciones a personal cualificado, registrar las incidencias, programar su mantenimiento…
- **Seguridad del equipo fuera de la organización**. Atender a los riesgos para la organización. En todo caso, el uso externo debe autorizarse por el equipo directivo. Y en cualquier caso, los equipos nunca serán desatendidos y se evaluarán los riesgos de dicho uso.

4.5. Cumplimiento

Este apartado recuerda la necesidad del cumplimiento del marco normativo y de todo requisito de seguridad que en él esté implícito. En esta misma línea de legalidad, la organización tenderá a optimizar esta efectividad a través del recurso de una auditoría sobre las infraestructuras y las aplicaciones.

- **Cumplimiento de los requisitos legales**. Garantía de control sobre cualquier violación de las disposiciones legales vigentes, los estatutos propios, los contratos o los requisitos de seguridad de la información. Se considerará que el diseño, la operación, el uso y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad. Se valorará la incorporación de asesores legales especializados en la materia, ya que la complejidad de cuestiones como son la propiedad intelectual, la protección de datos y la privacidad lo requieren. Sin olvidar que es responsabilidad de todas las áreas de la organización el conocimiento de la legislación vigente en sus respectivos ámbitos.
- **Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico**. Garantía del cumplimiento con las políticas y estándares internos de seguridad en la gestión de los sistemas de información. La evolución de las políticas de seguridad, la tecnología y los propios sistemas de información necesitarán de una revisión en el cumplimiento de los requisitos de seguridad.
- **Consideraciones de auditoría de los sistemas de información**. Garantía de maximizar la efectividad del proceso de auditoría y de minimizar las interferencias del propio sistema de información. Se considerará la existencia de controles durante el proceso de auditoría que salvaguarden la integridad de las herramientas de la auditoría y que prevengan de su mal uso.

4.6. Gestión de activos

La gestión de los activos tiene como objetivo responsabilizarse de los activos mediante una protección que incluya la identificación de los propietarios; también asegurar la clasificación, según un nivel adecuado de protección.

En cuanto a la responsabilidad de los activos, éstos deben identificarse y ser gestionados mediante el mantenimiento de unos controles adecuados.

- **Inventario de los activos**. La organización debe identificar los activos y documentar su importancia, para una mejor gestión en caso de desastres. No hay que duplicar innecesariamente otro tipo de inventarios, pero sí asegurar unos contenidos consolidados. La responsabilidad también debe documentarse.
- **Responsabilidad de los activos**. La información y los activos asociados con los medios de tratamiento deben ser responsabilidad de la organización que, como tal, debe velar por su correcta clasificación y definir y revisar sus restricciones. Aunque se delegue la custodia, la responsabilidad permanece en la organización propietaria.
- **Uso de los activos**. Todo aquel que se relacione con la información debe seguir unas pautas en su uso y sus activos asociados con los medios de tratamiento. Para ello, el equipo directivo promoverá reglas específicas.

En el campo de la clasificación se garantizará que la información recibe un nivel correcto de protección. Los activos se clasifican según su sensibilidad y criticidad para la organización. La información tiene grados de confidencialidad que se regularán en un esquema de clasificación, que marcará niveles de protección y difundirá las medidas especiales de uso.

- **Lineamientos de clasificación**. La información se clasificará según el valor, los requerimientos legales, la sensibilidad y la criticidad para la organización. Estos lineamientos incluirán protocolos de revisión. Toda clasificación debe ser ponderada y proporcionada.
- **Etiquetado y manejo**. La gestión de la información deberá ser concordante con su clasificación. El etiquetado reflejará la clasificación de acuerdo con los protocolos establecidos. A su vez, cada nivel de protección debe aparejar unos procedimientos de manejo determinados, incluyéndose el tratamiento, el almacenamiento, la transmisión, la desclasificación y la eliminación, si cabe. El etiquetado y manejo de la información son claves para el intercambio de información clasificada.

4.7. Gestión de comunicaciones y operaciones

Este apartado persigue garantizar una segura y controlada explotación de la infraestructura, con su pertinente supervisión y registro de incidencias. Para lo cual existe el propósito de controlar:

- **Procedimientos y responsabilidades operacionales**. Garantía de una correcta operación de los medios de tratamiento de la información, mediante el establecimiento de responsabilidades y procedimientos para la gestión y la operación de todos los medios de tratamiento.

- **Gestión de servicios de terceros**. Garantizar un nivel apropiado de seguridad tras acuerdos de entrega de servicios a terceros. Cabrá un chequeo y monitorización, por parte de la organización, de la implementación de los acuerdos y del cumplimiento de los estándares para asegurarse de que los entregables sean satisfactorios.
- **Planificación y aceptación de sistemas**. Minimizar el riesgo de fallas. La planificación asegurará la capacidad y la disponibilidad de los recursos necesarios. La proyección de capacidad futura prevendrá riesgo de sobrecarga con el tiempo. Todo sistema nuevo, antes de ser aceptado y utilizado, documentará y probará los requerimientos.
- **Protección contra códigos maliciosos**. Proteger la integridad del software con la toma de precauciones ante códigos maliciosos y códigos móviles no autorizados. El personal estará informado de los peligros y el equipo directivo introducirá controles para su eliminación.
- **Copias de seguridad**. Garantía de la integridad y la disponibilidad de la información y sus medios de tratamiento. Establecimiento de procedimientos de rutina para implementar el back-up y la estrategia de copias. También se ensayará la restauración.
- **Gestión de la seguridad de red**. Garantía de la protección de la información en redes y su infraestructura de soporte. Cabrá considerar cuestiones legales y monitoreo, además de un control adicional respecto de la información confidencial. Se debe vigilar una posible suplantación del emisor y una posible pérdida de información.
- **Gestión de dispositivos de almacenamiento**. Control de la divulgación no autorizada, la modificación o la interrupción de actividades. Cabrá un control y protección físicos.
- **Intercambio de información entre organizaciones**. Garantía de la seguridad en el intercambio de información y software, al respaldarse en una política formal seguida de líneas de acuerdos, así como del cumplimiento de las disposiciones legales vigentes.
- **Servicio de correo electrónico**. Garantía de seguridad en el servicio y su uso seguro. Cabrá considerar la integridad y la disponibilidad de la información publicada electrónicamente, así como las implicaciones de la seguridad asociada al correo electrónico.
- **Monitorización de sistemas**. Control sobre actividades de tratamiento de información no autorizadas. Cabrá el monitoreo de los sistemas y los informes de incidentes de seguridad de la información, además del propio chequeo de la efectividad de los controles.

4.8. Control de acceso

El control de acceso a los sistemas de información se considera uno de los campos cruciales en la seguridad de la información. En este campo se establecerán procedimientos de control que permitan el acceso según la política de la organización, con especial atención a los accesos privilegiados y al acceso de software malicioso.

- **Requisitos del negocio para el control del acceso**. Garantía del acceso a la información. Los requisitos de la organización marcarán y serán la base del acceso a la información. Las pautas de control del acceso respetarán la política de divulgación del propio organismo.
- **Gestión del acceso de los usuarios**. Garantía de un acceso autorizado a los sistemas de información y control ante el acceso no autorizado. Cabrán procedimientos formales

para controlar los derechos de acceso. Dichos procedimientos abarcarán todo el ciclo del acceso, desde el registro de nuevos usuarios hasta el borrado de aquéllos que ya no requieren acceso. Se tenderá a minimizar el acceso restringido a la información confidencial.

- **Responsabilidades del usuario**. Garantía de control ante accesos no autorizados y vigilancia ante el peligro que corre la información en su tratamiento. Cabrá concienciar a los usuarios autorizados de lo importante de su cooperación en la consolidación de la seguridad de la información. Los usuarios deben ser responsables parciales de la efectividad de los controles, por ejemplo mediante el correcto uso de sus claves secretas, personales e intransferibles, y una correcta atención de los equipos.
- **Control de acceso de red**. Garantía de control ante el acceso no autorizado a los servicios de las redes, internas y externas. El acceso autorizado a las redes no comprometerá la seguridad de los servicios, por lo que se vigilará la:
    a. Existencia de interfaces apropiadas
    b. Aplicación de mecanismos de autenticación adecuados
    c. Obligación del control de acceso del usuario a la información
- **Control de acceso del sistema operativo**. Garantía de control ante el acceso no autorizado a los sistemas operativos. Se considerará el uso de medios de seguridad para restringir el acceso a usuarios no autorizados. Estos medios deben ser capaces de:
    a. Autenticación de usuarios autorizados, según política de control de acceso definida.
    b. Registro de intentos, fallidos y exitosos, de autenticación del sistema.
    c. Registro del uso de privilegios especiales del sistema.
    d. Emisión de alarmas ante la violación de las políticas de seguridad del sistema.
    e. Proporcionar los medios de autenticación apropiados.
    f. Restricción, en su caso, del tiempo de conexión de los usuarios.
- **Control de acceso a las aplicaciones y a la información**. Garantía de control ante accesos no autorizados a la información de las aplicaciones. Se considerará el uso de medios de seguridad para la restricción del acceso a la información y a las aplicaciones. Las aplicaciones deberán estar capacitadas para:
    a. Control del acceso del usuario a la información y a las aplicaciones, según la política de control de acceso definida.
    b. Proporcionar protección ante accesos no autorizados al software del sistema de operación y de software malicioso que supere los controles del sistema.
    c. No comprometer a otros sistemas con los que se comparten recursos.
- **Teletrabajo y movilidad**. Garantía de la seguridad de la información ante el uso de medios móviles. La protección será proporcional al riesgo de estos modos de trabajo, como puedan ser los ambientes desprotegidos, en el caso de la movilidad, y la protección específica del lugar, en el caso del teletrabajo.

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

En este apartado se trata de garantizar la integridad de la seguridad de la información en los sistemas.

- **Requisitos de seguridad que afectan a los sistemas**. Garantía de que la seguridad forme parte integral de los sistemas de información. Los sistemas de información pueden incluir sistemas de operación, infraestructura o servicios, y aplicaciones desarrolladas por el usuario. Por ello, el diseño del sistema debe identificar y acordar requisitos de seguridad antes de su propio desarrollo.
- **Correcto tratamiento de las aplicaciones**. Garantía contra errores, pérdida, modificación no autorizada o mal uso de la información de las aplicaciones. Se considerará el diseño de controles adecuados en las aplicaciones, incluyendo una validación de los datos de entrada y de salida. Se aplicará especial atención al tratamiento de la información confidencial mediante controles adicionales.
- **Controles criptográficos**. Garantía de la confidencialidad, la autenticidad o la integridad por el uso de medios criptográficos. Se considerará el desarrollo de una política organizacional sobre los controles criptográficos, como refuerzo a una posible protección inadecuada por parte de otros controles.
- **Seguridad en los sistemas de ficheros**. Garantía de seguridad e integridad de los sistemas de ficheros. Se considerará el control del acceso a estos sistemas y del código fuente del programa.
- **Seguridad en los procesos de desarrollo y soporte**. Garantía para el mantenimiento de la seguridad del software y la información de las aplicaciones. Los responsables de las aplicaciones cobrarán responsabilidad sobre la seguridad de los proyectos y del soporte. Se estima básica la revisión de cualquier cambio que se proyecte sobre el sistema de información, para evitar colisionar con la seguridad.
- **Gestión de vulnerabilidades técnicas**. Garantía de reducción de riesgos sobrevenidos de la explotación de vulnerabilidades técnicas. La gestión de la vulnerabilidad técnica debe ser sistemática, confirmando su efectividad tras la obtención de la oportuna información de los sistemas de información.

4.10. Gestión de incidentes de seguridad de la información

En este apartado, se persigue garantizar que los registros de incidencias y las debilidades en la seguridad de la información y de sus sistemas se comuniquen de manera pertinente, como medio que posibilite la debida corrección.

- **Informe de los eventos y debilidades de la seguridad de la información**. Garantía de que una correcta comunicación de los eventos y debilidades de la seguridad, asociados al sistema, permiten medidas correctoras. Se considerará el establecimiento de procedimientos formales de informe, que afectarán a todo el personal de la organización. Se requerirá rapidez en la comunicación de aquellos informes de eventos que impacten en la seguridad de la información a través de los canales adecuados.
- **Gestión de los incidentes y mejoras en la seguridad de la información**. Garantía de aplicación de un enfoque consistente en la gestión de los incidentes de seguridad. Se considerará el establecimiento de responsabilidades y procedimientos para gestionar con eficacia los eventos y las debilidades de la seguridad. Cabrá un proceso de mejora continua para la respuesta al monitoreo, su evaluación y la gestión de incidentes.

4.11. Gestión de la continuidad del negocio

Este apartado considera la importante cuestión de la disponibilidad de la información que soportan las aplicaciones en caso de desastres. Para ello, el objetivo se centra en el establecimiento de un plan de acción que minimice los efectos de cualquier catástrofe. La organización debe saber responder a una interrupción en sus actividades, proteger sus procesos críticos y garantizar una pronta reanudación de sus funciones.

Se considerará la implementación de un proceso de gestión de la continuidad del negocio, que minimice impactos y permita una rápida recuperación de pérdidas de activos de información a niveles aceptables. El proceso deberá identificar procesos críticos e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio en otros requisitos de continuidad parciales.

Las consecuencias de los desastres merecen un análisis de su impacto en la organización. De lo que se deriva que la seguridad de la información deberá integrarse en el proceso general de continuidad de negocio en toda organización.

- **Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio**. Se considerará el desarrollo y el mantenimiento de un proceso integral para la continuidad del negocio, en toda la organización, que trate los requisitos de seguridad de la información.
- **Continuidad del negocio y evaluación del riesgo**. Se considerará la identificación de aquellos eventos que puedan interrumpir procesos de la organización, sopesando su impacto y sus consecuencias.
- **Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información**. Se considerará el desarrollo y la implementación de planes que aseguren la disponibilidad de la información en niveles aceptables y en plazos de tiempo razonables, en caso de interrupción del negocio.
- **Marco referencial de los planes de continuidad del negocio**. Se considerará la opción de mantener un único marco referencial en cuanto a los planes de continuidad del negocio, para que los planes parciales sean consistentes respecto de la seguridad de la información
- **Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio**. Los planes de continuidad del negocio serán debidamente probados y actualizados para asegurar su efectividad. Se considerará la designación de un responsable en las revisiones regulares de cada plan de negocio que, con un proceso formal de control de cambios parciales, dotará al plan completo de mayor consistencia y eficacia.

5. Cuadro de compromisos de cumplimiento

Este cuadro identifica aquellos compromisos establecidos en las líneas de actuación de la Guía de Implementación de Administración electrónica y unas recomendaciones sobre cómo cumplir con los mismos.

El número representado es el mismo con el que se identifica dicho compromiso en la Guía de Implementación.

Nª	Compromisos	Cómo cumplir con los compromisos
4.1	Adoptar una política de seguridad de la información	Elaborar, los equipos directivos, una política de seguridad de la información Publicar y difundir en la organización un documento que defina el marco de aplicación Revisar y actualizar el documento, en búsqueda de su mayor idoneidad, eficiencia y efectividad
4.2	Observar una buena gestión de los aspectos organizativos de la seguridad de la información, tanto de la participación interna como externa	A nivel interno: - Asumir, el equipo directivo, la importancia de la seguridad - Coordinar la seguridad - Asignar roles - Revisar con carácter independiente la seguridad A nivel externo: - Identificar los riesgos - Tratar la seguridad
4.3	Conocer y aceptar, el personal de la organización, la responsabilidad que conlleva la seguridad de la información	Para la selección de personal: - Definir los roles y responsabilidades - Incluir términos y condiciones de seguridad en el contenido de los contratos Para el personal interno: - Requerir a todo el personal la aplicación de la seguridad, según la política procedimientos establecidos. - Capacitar en materia de seguridad de la información y actualizar los conocimientos sobre políticas y procedimientos

Nª	Compromisos	Cómo cumplir con los compromisos
		Para el personal saliente: - Definir las responsabilidades tras el abandono del puesto en la organización - Devolver activos, quien pudiera tener en su posesión, bien software o documentos corporativos - Retirar derechos de acceso
4.4	Garantizar la protección física y ambiental de los activos físicos a través del control de acceso	Proteger las áreas seguras, donde se encuentran los medios de tratamiento de información crítica o confidencial - Proteger las áreas que contienen información y medios de tratamiento de información - Permitir el ingreso sólo a personal autorizado - Diseñar los lugares con especial control del acceso - Proteger contra amenazas externas e internas - Controlar el tránsito de personas externas
4.5	Cumplir el marco normativo y de todo requisito de seguridad que en él esté implícito	Cumplir con los requisitos legales, mediante el control sobre cualquier violación de las disposiciones legales vigentes, estatutos propios, contratos o requisito de seguridad de la información Cumplir con las políticas y estándares de seguridad y cumplimiento técnico Considerar auditorías de los sistemas de información
4.6	Gestionar los activos como medio para cobrar responsabilidad mediante una protección que incluya la identificación de los propietarios; también para asegurar la clasificación, según un nivel adecuado de protección	Identificar y gestionar los activos mediante el mantenimiento de unos controles adecuados: - Identificar los activos y documentar su importancia - Velar por su correcta clasificación y definir y revisar sus restricciones - Seguir unas pautas en el uso

Nª	Compromisos	Cómo cumplir con los compromisos
		Garantizar que la información recibe un nivel correcto de protección: - Clasificar de manera ponderada y proporcionada. - Etiquetar y manejar, para un mejor intercambio de información clasificada
4.7	Garantizar una segura y controlada explotación de su infraestructura, con una pertinente supervisión y registro de incidencias	Establecer los siguientes controles: - Establecer responsabilidades y procedimientos para la gestión y la operación de todos los medios de tratamiento - Chequear y monitorizar los servicios de terceros - Asegurar la capacidad y la disponibilidad de los recursos necesarios - Proteger la integridad del software con la toma de precauciones ante códigos maliciosos y códigos móviles no autorizados - Establecer procedimientos de rutina para implementar el back-up y la estrategia de copias - Gestionar la seguridad de red mediante el monitoreo y la consideración de cuestiones legales - Controlar y proteger físicamente los dispositivos de almacenamiento - Intercambiar la información entre organizaciones, como una política formal - Considerar la integridad y la disponibilidad de la información publicada electrónicamente - Monitorear los sistemas y los informes de incidentes de seguridad de la información

Nª	Compromisos	Cómo cumplir con los compromisos
4.8	Considerar el control de acceso a los sistemas de información como uno de los campos cruciales en la seguridad de la información	Establecer los siguientes controles: - Marcar los requisitos del negocio para el control del acceso - Controlar los derechos de acceso de los usuarios - Concienciar a los usuarios autorizados de lo importante de su cooperación en la consolidación de la seguridad de la información - Controlar el acceso no autorizado a los servicios de las redes, internas y externas - Usar medios de seguridad para restringir el acceso a usuarios no autorizados - Usar medios de seguridad para la restricción del acceso a la información y a las aplicaciones. - Proteger proporcionalmente ante el riesgo del teletrabajo y movilidad
4.9	Garantizar la integridad de la seguridad de la información en los sistemas	Establecer los siguientes controles: - Diseñar los requisitos de seguridad que afectan a los sistemas - Diseñar controles adecuados en las aplicaciones, incluyendo una validación de los datos de entrada y de salida - Desarrollar una política organizacional sobre los controles criptográficos - Controlar el acceso a los sistemas de ficheros y del código fuente del programa - Mantener la seguridad del software y la información de las aplicaciones. - Gestionar la vulnerabilidad técnica sistemáticamente
4.10	Garantizar que los registros de incidencias y las debilidades en la seguridad de la información y de sus sistemas se comuniquen de manera pertinente, como medio que posibilite la debida corrección	Establecer los siguientes controles: - Establecer procedimientos de informe, que afectarán a todo el personal de la organización. - Establecer responsabilidades y procedimientos para gestionar con eficacia los eventos y debilidades de la seguridad

Nª	Compromisos	Cómo cumplir con los compromisos
4.11	Implementar un plan de continuidad del negocio que responda a la interrupción de sus actividades y proteja sus procesos críticos, garantizando una pronta reanudación de sus funciones	Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio Asegurar la continuidad del negocio y una evaluación del riesgo Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información Establecer un marco referencial en los planes de continuidad del negocio Probar, mantener y reevaluar los planes de continuidad del negocio

6. Términos y referencias

6.1. Glosario

Activo de información: cualquier recurso de información o datos con valor para el desarrollo de las funciones de una organización, que puede ser comprendido y tratado como una única unidad a efectos de gestión, uso, protección e intercambio. Aunque puede designar piezas aisladas de información (una imagen incluida en un documento, un registro de una base de datos), suele emplearse para identificar y tratar conjuntos de información o datos, como agrupaciones documentales, bases de datos, sitios web, colecciones de metadatos… En el ámbito de la seguridad de la información se emplea también para designar el hardware y software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información.

Amenaza: causa potencial de un incidente no deseado, que puede provocar daño a un sistema o a una organización.

Autenticación: situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede verificar que es quien dice ser y, por ello, pasa a ser considerado un usuario autorizado.

Control: medio para gestionar un riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras de la organización, que pueden ser técnicas, de gestión o naturaleza legal. También puede ser sinónimo de salvaguarda.

Medios de tratamiento de la información: cualquier sistema, servicio o infraestructura de tratamiento de la información, o bien los locales físicos donde se alojan.

No repudio: servicio de seguridad, estrechamente relacionado con la autenticación, que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades: no repudio en origen y no repudio en destino. Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (véase *No repudio en origen*) y que el destinatario la recibió (véase *No repudio en destino*).

No repudio en destino: servicio de seguridad mediante el cual el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

No repudio en origen: servicio de seguridad mediante el cual el emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito

ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario

Plan de continuidad del negocio: plan de protección dirigido a la solución de los incidentes que provoquen una interrupción en la actividad de las organizaciones, reducir la probabilidad de que se produzcan y garantizar la recuperación de su empresa.

Riesgo: combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información, que también puede involucrar a otras propiedades como la autenticidad, la trazabilidad, el no repudio y la fiabilidad.

Vulnerabilidad: debilidad de un activo que puede ser explotada por una amenaza.

6.2. Referencias y bibliografía

ESPAÑA. 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. *Boletín Oficial de Estado* [en línea], 29 de enero de 2010, 25. [Consulta: 15 diciembre 2014]. Disponible en: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

ESPAÑA. GOBIERNO VASCO. 2010. *Manual de seguridad* [en línea]. Vitoria-Gasteiz: Departamento de Justicia y Administración Pública. [Consulta: 15 diciembre 2014]. Disponible en: https://euskadi.net/contenidos/informacion/bp_segurtasuna/es_dit/adjuntos/MSPLATEA_c.pdf

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2013. *ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements*. Ginebra: ISO.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). 2013. *ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls*. Ginebra: ISO.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE). 2004. *Directrices de la OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad* [en línea]. París: OCDE; Madrid: Ministerio de Administraciones Públicas. [Consulta: 15 diciembre 2014]. Disponible en: http://www.oecd.org/sti/ieconomy/34912912.pdf

UNIÓN EUROPEA. 2001. Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo [en línea]. *Diario Oficial de las Comunidades Europeas*, 11 de abril de 2001, L 101. [Consulta: 15 diciembre 2015]. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32001D0264&qid=1401793082125&from=EN

VILLALÓN HUERTA, A. 2004. Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799 [en línea]. En: *El Sistema de Gestión de Seguridad de la Información. La nueva norma UNE 71502, Valencia, España. Septiembre, 2004*. [Consulta: 15 diciembre 2014]. Disponible en: http://www.shutdown.es/ISO17799.pdf