NORMA DE USO DE SOPORTES DE ALMACENAMIENTO DE INFORMACIÓN

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

INTRODUCCIÓN **5**

2 ÁMBITO DE APLICACIÓN **5**

3 CONTEXTO DE LA PRESENTE NORMA **5**

4 TERMINOLOGÍA RELEVANTE **6**

5 PROVISIÓN DEL SERVICIO **7**

6 NORMAS DE USO GENERALES **8**

7 NORMAS DE USO DEL ALMACENAMIENTO EN RED **9**

7.1 Usos autorizados 9

7.2 Usos no autorizados 9

8 NORMAS DE USO DE LOS SOPORTES REMOVIBLES DE ALMACENAMIENTO **10**

9 NORMAS ADICIONALES PARA LA INFORMACIÓN EN PAPEL **11**

10 MEDIDAS DE CONTROL **12**

11 INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD **13**

12 REVISIÓN DE LA NORMA **13**

13 RESPONSABILIDAD POR INCUMPLIMIENTO **14**

14 ANEXO I: REFERENCIAS **14**

14.1 Medida org.2 14

14.2 Medida op.acc.1 15

14.3 Medida op.acc.4 17

14.4 Medida op.exp.6 17

14.5 Medida mp.eq.1 18

14.6 Medida mp.si.1 18

14.7 Medida mp.si.2 19

14.8 Medida mp.si.3 19

14.9 Medida mp.si.5 19

14.10 Medida mp.info 1 20

14.11 Medida mp.info.3 20

14.12 Medida mp.info 9 21

Cuadro Resumen del Documento

Tipo de Documento	Norma sobre responsabilidad de la información y criterios para su calificación
Autor	Oficina de Seguridad de la Información MUFACE
Fecha de elaboración	03/10/2025
Revisado por	Leonardo González García
Aprobado por	Silvia Lacleta (Responsable de Seguridad)

Control de Cambios

Versión	Fecha	Descripción de la modificación
1.0	03/10/2025	Versión inicial

1 Introducción

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de aplicación al sector público, según el artículo 2 de la Ley 40/2015 del 1 de octubre, y según el artículo 156.2, establece los principios básicos y requisitos mínimos requeridos para proteger la información. Las Administraciones Públicas deberán aplicarlo para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

MUFACE asigna al personal los equipos y sistemas de información básicos necesarios para la ejecución de las actividades laborales en el ámbito de sus competencias, en la medida de la disponibilidad de estos y con la aprobación de la autoridad respectiva, convirtiéndose estas personas en usuarios, responsables de estos recursos.

Para garantizar el uso racional y seguro de estos recursos, debe conocerse la norma donde se especifica qué se considera un uso correcto del servicio. Con ese objeto, se redacta el presente documento, que describe la Norma de uso de soportes de almacenamiento de información.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (internos y externos) que tengan acceso a los soportes de almacenamiento gestionados por MUFACE.
En concreto este documento describe las normas de utilización de los soportes de almacenamiento, utilizados por los usuarios para albergar información en formato electrónico: almacenamiento local, carpetas en red, dispositivos removibles (USBs, CDs/DVDs, discos duros externos, ...), etc.

3 Contexto de la presente norma

La presente norma de uso de los soportes de almacenamiento pertenece a una serie de documentos que describen la normativa de uso seguro de los recursos informáticos de MUFACE, relacionada con la seguridad en los puestos de trabajo, la red corporativa, los

equipos portátiles, las aplicaciones informáticas, así como sobre el acceso y tratamiento de la información por parte de los usuarios.

La citada serie de documentos se integran a su vez dentro del desarrollo normativo de seguridad derivado de la Política de Seguridad de la Información (PSI) de MUFACE, que está alineado con los principios básicos y los requisitos mínimos exigidos por el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS).

El *Responsable de Seguridad* aprobará los procedimientos específicos que sean necesarios para el desarrollo de esta norma.

4 Terminología relevante

A lo largo del texto de los documentos de desarrollo normativo de seguridad requeridos por la PSI de MUFACE se citan una serie de definiciones, entre ellas algunas figuras o roles, a los que se aludirá con letra cursiva siguiendo la siguiente nomenclatura:

- **Usuario:** la persona o sistema que utiliza los sistemas de información de MUFACE, y/o a la información contenida en ellos.
- **Unidad TIC**: unidad encargada del desarrollo, mantenimiento y explotación del sistema de información al que estemos haciendo referencia.
- **Responsable del Sistema**: según define la PSI, esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes. Por tanto, según esta definición, recae sobre el titular de la Unidad TIC.
- **Responsable de Seguridad**: según define la PSI, la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios.
- **Norma específica de cada ámbito:** Una norma específica desarrolla con mayor detalle la norma correspondiente de aplicación general dentro del ámbito de competencia de cada Responsable de Seguridad, si se considera necesario por parte de éste. En caso de existencia de norma específica y de discrepancia entre ésta y la norma general, prevalecerá lo indicado en la específica para la información y servicios afectados por los sistemas de información gestionados por el ámbito de competencia del Responsable de Seguridad correspondiente.

5 Provisión del servicio

MUFACE pone a disposición de los usuarios medios de almacenamiento de información para el cumplimiento de sus obligaciones, como pueden ser las unidades o carpetas en red o ciertos soportes removibles. Dichos medios no están destinados al uso personal o extraprofesional de los usuarios, los cuales deben conocer que no gozan de un uso privativo del mismo.

Deberá tenerse en cuenta además que ciertos recursos, como el servicio de almacenamiento de información en la red, son limitados y compartidos con otros usuarios.

El acceso a la red de almacenamiento de datos debe hacerse desde un equipo debidamente registrado y/o autorizado por la *Unidad TIC* que presta el servicio de almacenamiento y mediante la utilización de un usuario debidamente identificado.
Podrán existir carpetas en red individuales o compartidas de grupo, con posibilidad de establecer cuotas u otras restricciones de espacio en ambos casos. También se podrán ofrecer carpetas temporales para intercambio de ficheros cuyos contenidos se borrarán periódicamente.

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización.

La copia de seguridad periódica de la información alojada en la red de almacenamiento de datos es responsabilidad de la *AEAD* que presta el servicio de almacenamiento. Se realizarán copias de seguridad de las carpetas en red individuales y de grupo, pero no de las de intercambio de ficheros u otras que puedan existir de carácter temporal. Tampoco se realizarán copias de ficheros multimedia (música, imágenes, vídeos, etc.) almacenados en red, salvo en aquellos directorios expresamente autorizados.

Cada usuario será responsable de la integridad y copia de seguridad tanto de la información almacenada localmente en el ordenador que tenga asignado, como la almacenada en los soportes removibles de los que disponga.

Con la finalización de la relación de servicio con MUFACE por parte de un usuario se interrumpirá su acceso al almacenamiento local y en red.

La AEAD procederá al borrado seguro de la información almacenada en las carpetas de red individuales correspondientes al usuario cuya relación de servicio con MUFACE ha finalizado, previamente a su reutilización y asignación a nuevos usuarios, según el procedimiento establecido para ello. Asimismo, procederá a la destrucción segura de los soportes de almacenamiento utilizados cuando estos lleguen a su fin de vida útil, utilizando para ello, preferentemente, productos certificados. Se entiende por borrado y destrucción seguras aquellas que garantizan que no se pueda recuperar información que ha sido eliminada del sistema.

6 Normas de uso generales

Está terminantemente prohibido almacenar cualquier tipo de ficheros (documentos, imágenes, contenidos multimedia, etc.) con contenido intimidatorio, ofensivo, provocador, violento, amenazador, obsceno o, en general, que atente contra la dignidad de la persona.

No está permitido almacenar contenidos que incumplan la legislación de derechos de autor y propiedad intelectual.

Se deberá cumplir la legislación de datos de carácter personal *Reglamento 679/2016 y Ley Orgánica 3/2018)*.
Aplicando el principio básico del ENS de seguridad por defecto, los derechos de acceso de cada usuario a los sistemas de almacenamiento, se limitarán atendiendo a los siguientes principios:

- Mínimo privilegio, los derechos de acceso se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.
- Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones

Está prohibida cualquier actuación que pueda poner en riesgo la seguridad de la información manejada, en cuanto a que pueda suponer un menoscabo de su confidencialidad, integridad o disponibilidad.

7 Normas de uso del almacenamiento en red

7.1 Usos autorizados

1. Los contenidos almacenados se restringirán a ficheros relacionados con la actividad laboral del usuario.
2. Para poder acceder al almacenamiento el usuario deberá autenticarse previamente presentando sus correspondientes credenciales de acceso.

7.2 Usos no autorizados

1. Almacenar en las unidades de red archivos (especialmente los de música, imágenes, videos y similares) con fines que están fuera del ámbito de las actividades del Ministerio.
2. Almacenar ficheros infectados por virus o cualquier tipo de software malicioso (malware) por actuación voluntaria o negligente. No se deberán subir ficheros al almacenamiento local o en red sin analizarlos previamente con el software antivirus corporativo.
3. Realizar intentos de acceso a contenidos pertenecientes a otro usuario sin el permiso expreso y por escrito del mismo.
4. Realizar intentos de acceso a contenidos pertenecientes a un grupo al que no pertenece el usuario, sin el permiso expreso y por escrito de un superior jerárquico del que dependan todos los componentes del grupo.

8 Normas de uso de los soportes removibles de almacenamiento

Los dispositivos removibles de almacenamiento representan un punto vulnerable para los recursos informáticos y la posible pérdida o robo de información, debido a lo generalizado que está su uso y a su facilidad de conexión.

Se consideran dispositivos removibles de almacenamiento los discos duros externos, CDs, DVDs, tarjetas de memoria, dispositivos de memoria USB / FireWire, smartphones, PDAs y cualquier otro dispositivo disponible en el mercado que pueda ser utilizado con finalidad de recuperar y almacenar información y que pueda ser transportado con facilidad. También se considerarán como tal, a efectos de la presente normativa, los discos duros de los ordenadores portátiles.

La utilización de dispositivos removibles en los que sea posible la escritura de información (memorias, etc.) únicamente estará autorizada en el caso de que dichos soportes tengan un uso exclusivo para la conexión con equipos corporativos o en equipos que aseguren un nivel de seguridad al menos equivalente al de los equipos corporativos.

En los casos en los que sea necesario el etiquetado de los soportes removibles de información, se realizará de forma que no revele su contenido.

No está permitido almacenar información sensible o confidencial, salvo autorización expresa del responsable de dicha información.

Asimismo, no está permitido almacenar datos de carácter personal salvo autorización expresa del responsable del fichero y con las consideraciones indicadas en el apartado de Normas de uso generales.

En cualquiera de los dos últimos casos, si existiera la citada autorización para almacenar la información en el soporte removible, el usuario deberá mantenerla cifrada para evitar su revelación en caso de extravío o robo del dispositivo. El personal de la *Unidad TIC* que presta soporte informático al usuario proporcionará las herramientas de cifrado autorizadas para tal efecto.

Es necesario llevar a cabo un borrado seguro con anterioridad a la reutilización de los dispositivos removibles ó cuando haya llegado al fin de su vida útil, especialmente en el caso de que haya contenido datos sensibles. Si la naturaleza del soporte no permite un borrado seguro, deberá ser destruido de forma segura. En ambos casos se emplearán, preferentemente, productos certificados.

El usuario es responsable de la información almacenada en los dispositivos removibles, y por tanto de la custodia del propio dispositivo.

Por tanto, deberá guardar el soporte en lugares seguros (armarios protegidos por llave, cajas de seguridad en hoteles, etc.) cuando no estén en uso.

Asimismo, el usuario deberá revisar con el antivirus cualquier dispositivo removible que se conecte al equipamiento que tiene asignado, para detectar posibles amenazas conocidas.

Está expresamente prohibida la conexión / habilitación de dispositivos removibles que faciliten la transferencia de información de manera inalámbrica que no reúnan los requisitos de seguridad mínimos que garanticen la confidencialidad de la información.

No se deben reutilizar para cualquier otro uso los soportes removibles que han almacenado previamente información sensible sin asegurarse de que dicha información ha sido destruida o sobreescrita de manera segura (borrado seguro).

9 Normas adicionales para la información en papel

Se debe mantener despejado el escritorio de trabajo de documentos impresos con información sensible en ausencia por largos periodos de tiempos o al finalizar el horario laboral.

Se deben destruir con regularidad todos aquellos documentos impresos que ya no sean necesarios a través de los procedimientos que establezca MUFACE (trituradora de papel, servicio de contenedores autorizados de reciclaje).

Se deben resguardar en lugares seguros (cajones y armarios bajo llave) los documentos impresos que contengan información sensible.

No está permitido imprimir datos de carácter personal salvo autorización expresa del responsable del fichero y siempre y cuando sean necesarios para el desempeño de sus funciones.

10 Medidas de control

MUFACE se reserva el derecho de aplicar las medidas técnicas y organizativas necesarias para garantizar el buen uso y la seguridad de sus sistemas de información.

En ese sentido, si se aprecia la existencia de riesgos importantes podrá tomar medidas tales como la deshabilitación o bloqueo de los puertos USB, de las ranuras para tarjetas de memoria, de los dispositivos de grabación CD / DVD o de cualquier otro puerto de conexión para dispositivos removibles de almacenamiento, que podrá aplicar tanto a equipos concretos como de forma generalizada.

En el caso específico del almacenamiento en red:

- Al no estar autorizado el almacenamiento de archivos de música, imágenes, videos y similares con fines ajenos al ámbito de las actividades del Ministerio, en caso de que se conozca la existencia de este tipo de ficheros la *Unidad TIC* que presta el servicio tendrá la facultad de eliminarlos sin necesidad de consultar al usuario.
- Si se sobrepasan las cuotas asignadas o se presentan problemas de almacenamiento disponible en los servidores, la *Unidad TIC* podrá, previo aviso al usuario o grupo de usuarios afectados, proceder a borrar los ficheros más antiguos, aparte de no permitir la inclusión de nuevos ficheros.
- Por motivos de seguridad y eficiencia en el uso del espacio del almacenamiento en red, la *Unidad TIC* podrá tomar medidas en base a las características de los ficheros almacenados (tipo de extensión, tamaño, etc.), tales como: impedir el almacenamiento, realizar el borrado periódico de los mismos, habilitar directorios específicos con políticas de retención distintas a la general, etc. Dichos criterios y medidas serán públicos, de modo que puedan ser conocidospor los usuarios.
- En caso de detectarse el incumplimiento de la presente norma, o de presentarse incidentes de seguridad derivados del mal uso del servicio de almacenamiento en

red, se podrá acordar la supresión o limitación del servicio a los usuarios involucrados.

- La *Unidad TIC* responsable del mantenimiento de las carpetas podrá dictar las condiciones e instrucciones de uso concretas que garanticen el cumplimiento de los principios establecidos en esta norma.

No se realizará la inspección manual de los contenidos de los ficheros almacenados, salvo que:

- Sea solicitado a la SEAP por las autoridades competentes bajo la investigación de una posible comisión de delitos.
- Sea solicitado por parte del propio usuario.
- Se detecte que contienen virus o malware, en cuyo caso la *Unidad TIC* correspondiente podrá tomar las acciones de protección que considere oportunas.

11 Información sobre incidentes de seguridad

El usuario deberá informar sobre cualquier incidente que considere relevante y que pueda afectar a la seguridad física o lógica, tanto los relacionados con los servicios electrónicos (correo electrónico, acceso a Internet, etc) como los relacionados con el equipamiento informático (hardware, software, dispositivos externos). Para ello utilizará los medios habilitados por MUFACE para la notificación de incidencias especificados en la intranet correspondiente y, en casos de gravedad, deberá también avisar a su superior inmediato.

Como ejemplos de posibles incidentes: sustracción o pérdida de soportes de almacenamiento removibles, detección de infección en los contenidos, sospechas fundadas de accesos no autorizados, etc.

12 Revisión de la norma

La presente norma y cualquier modificación a la misma, entrará en vigor en el momento en que sea aprobada por el Comité de Seguridad de la Información de MUFACE, lo que se notificará oportunamente mediante su publicación en la Intranet de MUFACE.

Las modificaciones totales o parciales de la presente normativa, así como la referencia de los documentos o versiones que sustituyen a este documento serán registradas mediante control de cambios y versión del documento.

13 Responsabilidad por incumplimiento

Todos los usuarios de los soportes de almacenamiento de MUFACE están obligados al cumplimiento de las pautas de conducta establecidas en la presente norma, pudiéndose derivar de su incumplimiento la pertinente responsabilidad en el ámbito disciplinario, si a ello hubiera lugar en aplicación de las disposiciones reguladoras del estatuto jurídico del usuario. La detección de actuaciones irregulares, ilícitas o ilegales podrá acarrear la iniciación de las medidas disciplinarias oportunas y, en su caso, de las acciones legales correspondientes.

14 Anexo I: Referencias

Se deberán tomar en consideración los siguientes textos y normativas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- PSI Política de Seguridad de la Información de MUFACE.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-800: Esquema Nacional de Seguridad - Glosario de Términos y Abreviaturas
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-804: Esquema Nacional de Seguridad. Guía de implantación.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-808: Verificación del Cumplimiento de las Medidas en el ENS.

Las directrices estipuladas en esta norma se fundamentan en los requisitos establecidos en el ENS que se mencionan a continuación.

14.1 Medida org.2

Se dispondrá de una serie de documentos que describan:

- El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

- Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

14.2 Medida op.acc.1

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

- La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

- Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.
- Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

14.3 Medida op.acc.4

Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.

Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.

Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.

Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.

El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

- Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

14.4 Medida op.exp.6

Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.

Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.

Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.

Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.

El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

- Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

- Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

14.5 Medida mp.eq.1

Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

- *Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.*

14.6 Medida mp.si.1

Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

14.7 Medida mp.si.2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga.

- Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
- Se emplearán algoritmos y parámetros autorizados por el CCN.

14.8 Medida mp.si.3

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).

Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

14.9 Medida mp.si.5

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

- Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

14.10 Medida mp.info 1

Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

14.11 Medida mp.info.3

Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.

La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.

El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

14.12 Medida mp.info 9

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.

Los procedimientos de respaldo establecidos indicarán:

a) Frecuencia de las copias.
b) Requisitos de almacenamiento en el propio lugar.
c) Requisitos de almacenamiento en otros lugares.
d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

- Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.