NORMA DE USO Y PROVISIÓN DEL EQUIPAMIENTO INFORMÁTICO

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

1 INTRODUCCIÓN 4

2 ÁMBITO DE APLICACIÓN 4

3 CONTEXTO DE LA PRESENTE NORMA 5

4 TERMINOLOGÍA RELEVANTE 5

5 PROVISIÓN DEL SERVICIO 6

6 NORMAS DE USO 7

6.1 Usos autorizados 7

6.2 Usos no autorizados 8

7 MEDIDAS DE CONTROL 10

8 INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD 11

9 REVISIÓN DE LA NORMA 11

10 RESPONSABILIDAD POR INCUMPLIMIENTO 12

11 ANEXO I: REFERENCIAS 12

11.1 Medida org.2 12

11.2 Medida op.acc.1 13

11.3 Medida op.exp.4 14

11.4 Medida op.exp.5 15

11.5 Medida op.exp.6 16

11.6 Medida mp.eq.2 16

11.7 Medida mp.eq.3 17

11.8 Medida mp.info.1 17

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 los mismos 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 y provisión del equipamiento informático.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (interno y externo) que tengan acceso a los sistemas de información gestionados por MUFACE.

En concreto este documento describe las normas de utilización del equipamiento informático utilizado para acceder a dichos sistemas de información: ordenadores personales de sobremesa (PCs), equipos portátiles (ordenadores portátiles, etc.), y equipamiento auxiliar del puesto de trabajo (impresoras, escáneres, faxes, etc.). No se consideran los dispositivos móviles (smartphones, tabletas, etc.), para los que se aplicará lo que se disponga en la norma que regula su uso.

3 Contexto de la presente norma

La presente norma de uso del equipamiento informático 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* correspondiente 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

La provisión de todo el equipo informático que utilizan para el desempeño de sus funciones el personal (interno y, si aplicara, el externo) de MUFACE, lo provee la Agencia Estatal de Administración Digital (AEAD).

La Unidad TIC de MUFACE, realizará labores de mantenimiento y gestión continua (tal y como se ha recogido en la normativa interna desarrollada por MUFACE) de los componentes del sistema, de forma que se puedan adaptar a nuevas necesidades previamente autorizadas y se reaccione y se proteja en lo posible a vulnerabilidades conocidas. De igual manera, se efectuará un seguimiento de las indicaciones de los fabricantes respecto a los defectos o vulnerabilidades que se van detectando y a las actualizaciones de seguridad, parches o nuevas versiones que ofrezcan como solución. Se evaluará la conveniencia de su aplicación en función del riesgo para la organización y la mitigación del mismo proporcionada por dicha aplicación, la posibilidad de ocasionar nuevos errores en aplicaciones existentes y la criticidad de éstas y la priorización de tareas según los recursos disponibles en cada momento determinado.

En relación con el equipamiento portátil, la posibilidad de que estos equipos se utilicen fuera del entorno de seguridad de la red corporativa de MUFACE se traducirá en la instalación y configuración de mecanismos de seguridad específicos (cortafuegos personales, cifrado de disco, etc), cuyas instrucciones de manejo se indicarán al usuario a la recepción del dispositivo, esto será gestionado por la Unidad TIC de MUFACE.

Al finalizar la relación de servicio con MUFACE por parte de un usuario deberá devolver el equipamiento que le fue asignado.

En relación con el borrado seguro, desde MUFACE se enviarán los equipos a la AEAD que será la responsable del borrado de los mismos siguiendo los requisitos que se establecen en el ENS.

6 Normas de Uso

6.1 Usos autorizados

1. El uso del equipamiento es para asuntos relacionados con el desempeño de las funciones que correspondan al puesto de trabajo que desempeña el usuario.
2. Los usuarios se limitarán a trabajar con los equipos que le han sido asignados o cuyo uso ha sido previamente autorizado, y en caso de requerir más recursos deberán solicitarlos a través de los canales establecidos a tal efecto.
3. En el caso de dispositivos portátiles, una vez entregado el dispositivo al usuario, se convierte en responsable de su custodia y protección ante accesos no autorizados, sustracciones o daños por manipulaciones incorrectas de terceros.
4. Por tanto, deberá guardar el equipamiento asignado en lugares seguros (armarios protegidos por llave, cajas de seguridad en hoteles, etc.) cuando no estén en uso.
5. Los equipos informáticos sólo podrán ser abiertos físicamente por el personal autorizado de la *Unidad TIC* correspondiente.
6. El software corporativo se utilizará siguiendo las normas, instrucciones o indicaciones de uso emitidas por la *Unidad TIC* correspondiente.
7. El acceso a la sesión del equipo se realizará mediante la introducción de las credenciales propias del usuario, que son individuales y deberán protegerse adecuadamente, no debiendo ser reveladas a terceras personas. MUFACE se reserva el derecho de utilizar otros mecanismos de autenticación fuerte, como los basados en certificados personales o cualquier otro método que se considere oportuno.
8. El usuario es responsable de asegurarse de mantener el bloqueo de sesión de manera manual en ausencia, por largos periodos de tiempos, del puesto trabajo.
9. Deberá tener especial cuidado de que, ante la posibilidad de pérdida o sustracción, los dispositivos portátiles estén siempre en situación de bloqueo protegido por contraseña cuando no estén siendo utilizados.

10. Al abandonar el puesto de trabajo deben cerrarse las sesiones establecidas con las aplicaciones, y apagar los equipos al finalizar la jornada laboral excepto en aquellos casos que estén expresamente autorizados.
11. En el caso de los dispositivos portátiles, deberán utilizarse únicamente los métodos autorizados, tanto para la conexión remota a la red interna como la conexión a otras redes como Internet.
12. Para el tratamiento de la información, se respetará en todo momento la legislación de protección de datos personales y las indicaciones incluidas en la *"Norma de uso de soportes de almacenamiento"*.
13. No podrá escanearse o fotocopiarse información generada o perteneciente a otro usuario sin el permiso expreso de éste.
14. Se debe retirar inmediatamente de las impresoras o faxes la información sensible o confidencial generada en formato papel.
15. Los usuarios deberán cumplir cualquier otra norma, instrucción o procedimiento de seguridad emitida por MUFACE.

6.2 Usos no autorizados

1. Emplear el equipamiento sin una autorización formal por parte de la Unidad TIC.
2. Transportar equipamiento informático fuera de las instalaciones de MUFACE.
3. Manipular los equipos de modo negligente o que dañe o destruya los equipos, o sus conexiones eléctricas y de datos. En ningún caso se podrá acceder físicamente al interior de los PCs, salvo el personal técnico autorizado para realizar operaciones de instalación, reparación o mantenimiento
4. Conectar a los equipos dispositivos externos o periféricos no autorizados por la Unidad TIC correspondiente.
5. Manipular alimentos y bebidas cerca de los equipos que puedan originar directa o indirectamente su mal funcionamiento.
6. Instalar en los equipos ningún tipo de software sin la autorización de la Unidad TIC, y muy especialmente software que no cumpla con las condiciones de licenciamiento o uso exigibles legalmente.
7. Desinstalar software, borrar archivos del sistema, o cambiar configuraciones de los equipos y programas sin la autorización y supervisión de la Unidad TIC.

8. No respetar la legislación de derechos de autor y propiedad intelectual en el software o material en formato electrónico utilizado en los equipos.
9. Realizar acciones tales como ejecutar software, visualizar salvapantallas, y abrir o reproducir cualquier tipo de ficheros (documentos, imágenes, contenidos multimedia, etc.) que den como resultado una actuación intimidatoria, ofensiva, provocadora, violenta, amenazadora, obscena o, en general, que atente contra la dignidad de la persona.
10. Introducir voluntariamente o debido a un comportamiento negligente virus o cualquier otro software malicioso susceptibles de causar alteración o daño sobre los sistemas de información y/o la información en ellos almacenada.
11. Desactivar el software antivirus o sus actualizaciones, o cualquier mecanismo de seguridad instalado en el equipo.
12. Conectar a la red equipos que no reúnan las suficientes garantías de seguridad según las pautas dictadas desde las Unidades TIC correspondientes.
13. Cualquier actuación que pueda poner en riesgo la confidencialidad de la información manejada, tales como la instalación o uso de:
    a. Software de espionaje (Spyware).
    b. Software o dispositivos de monitorización de tráfico, salvo en las Unidades TIC correspondientes, en el marco de actuaciones necesarias para la resolución de problemas o la optimización de las redes de comunicación.
    c. Software o dispositivos destinados a interceptar los datos de autenticación del usuario por cualquier método.
    d. Software o dispositivos destinados a intentar descubrir y acceder a recursos a los que no se les ha permitido expresamente el acceso.
    e. Programas P2P (“Peer to peer”) o de cualquier otro tipo que permita la compartición de información de manera no controlada.

    El usuario deberá tener especial atención en que los envíos de información al exterior de la SEAP se realicen a usuarios autorizados a conocer la información, y de que la información sensible vaya protegida mediante cifrado.

14. Realizar acciones destinadas a modificar, reubicar o sustraer la configuración física del equipo o de sus periféricos, para alterar o falsificar de manera fraudulenta su contenido.

15. Uso del equipamiento con fines comerciales o de obtención de lucro económico.

16. Permitir conexiones desde el exterior al equipo mediante mecanismos no autorizados por el *Responsable de Seguridad* correspondiente.

17. La conexión de equipos a la red corporativa sin las autorizaciones pertinentes, reguladas en la *"Norma de autorización y acceso a los Sistemas de Información"*.

18. Conectar los dispositivos portátiles a redes no autorizadas, como pueden ser las redes domésticas ó las redes inalámbricas no proporcionadas por MUFACE.

19. Respecto a la impresión en papel, en general no está permitido imprimir información no relacionada a las actividades de MUFACE. Además, se procurará no imprimir información confidencial salvo casos totalmente necesarios, debiendo en ese caso extremarse la precaución para proteger su confidencialidad.

20. Incumplir cualquier otra norma, instrucción o procedimiento relacionado con el uso del equipamiento software y hardware emitida por MUFACE.

21. Y cualquier otro comportamiento que dañe o menoscabe la seguridad o integridad de los sistemas de información de MUFACE y de la información en ellos contenida.

7 Medidas de control

MUFACE se reserva el derecho de aplicar las medidas técnicas y organizativas necesarias para garantizar el buen uso del equipamiento.

En este sentido, debe tenerse en cuenta que, cuando se considere necesario, las *Unidades TIC* de MUFACE tendrán la facultad de gestionar, controlar, configurar, auditar (su uso y software instalado), desmantelar o reubicar los equipos según lo consideren conveniente, para garantizar su mejor uso y aprovechamiento, con la debida justificación.

Podrá monitorizarse la actividad de los equipos asignados a los usuarios cuando se sospeche la realización desde ellos de actuaciones no autorizadas.

Se podrán tomar las medidas técnicas oportunas que limiten la conectividad de los equipos a periféricos externos o a redes no confiables (bloqueo de puertos USBs o unidades de CD/DVD, limitación de conexiones de red, etc). De igual manera, se podrá

restringir el acceso a la red a los equipos que no reúnan suficientes garantías hasta que sean subsanadas sus deficiencias de seguridad.

Cualquier aplicación o software instalado en los equipos que no cumpla con lo indicado en este documento podrá ser desinstalado sin aviso previo, sin que ello origine ninguna responsabilidad del personal de la *Unidad TIC* encargado de hacerlo.

En caso de detectarse el incumplimiento de la presente norma, o de originarse incidentes de seguridad derivados del mal uso del equipamiento, se podrá acordar la retirada de la autorización de uso de dicho equipamiento a los usuarios involucrados, e incluso su desconexión de la red corporativa. En el caso de dispositivos portátiles se podrá exigir la inmediata devolución de los mismos.

8 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 especificados en la intranet correspondiente y, en casos de gravedad, deberá también avisar a su superior inmediato.

Como caso de particular relevancia por su potencial riesgo para la seguridad de la información, la sustracción o pérdida de equipamiento portátil deberá comunicarse de manera inmediata. En el caso de sustracción dicha comunicación deberá acompañarse con la correspondiente denuncia policial.

9 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.

10 Responsabilidad por incumplimiento

Todos los usuarios de equipos y sistemas informáticos 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.

11 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.

11.1 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.

11.2 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.

11.3 Medida op.exp.4

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

- Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
- Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
- El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

- Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

11.4 Medida op.exp.5

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

- Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
- La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
- Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
- Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.

- Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

11.5 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.

11.6 Medida mp.eq.2

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

11.7 Medida mp.eq.3

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

- Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
- Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.
- Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.
- Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

11.8 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