NORMA DE USO Y PROVISIÓN DE DISPOSITIVOS MÓVILES

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 5

3 CONTEXTO DE LA PRESENTE NORMA 5

4 VIGENCIA 6

5 TERMINOLOGÍA RELEVANTE 6

6 PROVISIÓN DEL SERVICIO 7

6.1 Recursos corporativos 8

6.2 Recursos no corporativos 9

7 NORMAS DE USO 10

7.1 Usos autorizados 11

7.2 Usos no autorizados 11

7.2.1. Manipulación no autorizada de los recursos de movilidad: 11

7.2.2. Conexión con redes públicas no seguras 12

7.2.3. Almacenamiento de información y configuración no autorizados 12

10 REPORTE DE INCIDENTES DE SEGURIDAD 15

11 REVISIÓN DE LA NORMA 16

12 RESPONSABILIDADES 16

13 ANEXO I: REFERENCIAS 17

13.1 Medida mp.eq.3 – Protección equipos portátiles 17

13.2 Medida mp.si.2 - Criptografía 18

13.3 Medida mp.si.3 - Custodia 18

13.4 Medida mp.si.5 – Borrado y destrucción 19

13.5 Medida mp.info.1 – Datos de carácter personal 19

13.6 Medida mp.info.3 – Protección de dispositivos portátiles 19

13.7 Medida mp.info.6 – Copias de seguridad 20

Cuadro Resumen del Documento

Tipo de Documento	Norma de uso y provisión de dispositivos móviles
Autor	Oficina de Seguridad de 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.

En este sentido, desde MUFACE se 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.

De la misma forma, MUFACE podrá permitir, con las condiciones marcadas en el apartado 6.2 de esta norma, el uso de dispositivos no corporativos para la ejecución de las actividades laborales en el ámbito de sus competencias, previo consentimiento y aceptación expresa por parte del usuario de las medidas de seguridad.

Uno de los principios básicos establecidos en el Esquema Nacional de Seguridad (ENS) es el de gestión integral de la seguridad, incluyendo como un elemento importante, tal como indica el Artículo 6 del Real Decreto 311/2022, de 3 de mayo, los elementos humanos que intervienen en el proceso, así como a sus responsables jerárquicos *"para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad"*.

El uso de dispositivos móviles deberá ser responsable y acorde a las normas dictadas por MUFACE para mejorar la productividad de sus usuarios.

Tanto MUFACE como sus empleados tienen que tener en cuenta la importancia de la información que pueden contener los dispositivos móviles, tanto por el valor y la criticidad de la información corporativa, como por la información personal que contienen.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (tanto internos como externos) que tengan acceso a los recursos de movilidad de los sistemas de información gestionados por MUFACE.

En concreto este documento describe las normas de utilización de los distintos elementos y dispositivos de comunicaciones móviles: teléfonos móviles, smartphones, tabletas, módems USB, etc., así como de las líneas y tarjetas SIM que dotan de acceso a las redes de comunicaciones móviles a dichos dispositivos.

No se consideran los ordenadores portátiles, para los que se aplicará lo que se disponga en la norma de uso y provisión del equipamiento informático.

Los dispositivos móviles, como elementos de soporte removibles de almacenamiento, así como las memorias auxiliares que puedan albergar (tarjetas SD, etc.), están sujetos a la norma de uso de soportes de almacenamiento de información.

Serán igualmente aplicables tanto las normas de uso del correo electrónico corporativo y norma de acceso a Internet, como la norma de transmisión de la información en cuanto al acceso remoto desde dispositivos móviles.

3 Contexto de la presente norma

La presente norma de uso y provisión de dispositivos móviles pertenece a una serie de documentos que describen la normativa de uso seguro de los recursos informáticos de MUFACE, que se integran a su vez dentro del cuerpo normativo de la Política de Seguridad de la Información (PSI) de MUFACE, desarrollado para garantizar la seguridad de la información.

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

4 Vigencia

El presente documento es efectivo desde la fecha de aprobación, indicada en la segunda página del presente documento, y hasta que sea reemplazado por una nueva versión.

Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento.

En cualquier caso, toda la información referente a versiones, modificaciones, etc., aparece descrita en la ficha de versiones al inicio del documento.

5 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 de Seguridad**: según define la PSI, la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios.
- **Recurso de movilidad:** Todos aquellos dispositivos móviles y elementos que permiten el acceso en movilidad (teléfonos móviles, Smartphone, tablets, módems usb, tarjetas SIM, líneas de telefonía móviles, etc.).

  Se diferencian dos tipos de recursos de movilidad según su pertenencia:

  - **Recursos corporativos:** Son los recursos que han sido proporcionados a un usuario por MUFACE.
    - **Recursos no corporativos**: Son los recursos que no han sido proporcionados por MUFACE. Ésta no contrae ningún tipo de obligación para con los recursos personales de los empleados, independientemente de que éstos se utilicen para uso corporativo.

- **Uso Corporativo:** Se entiende por uso corporativo de los recursos aquellas acciones que dan como resultado que el empleado realice su trabajo dentro de MUFACE. Entre el uso corporativo cabe destacar:
    - Acceso y uso de aplicaciones corporativas.
    - Acceso y uso de información corporativa.
    - Acceso y uso del correo electrónico corporativo.
    - Acceso a documentos corporativos.
    - Acceso a servicios corporativos.
    - Comunicaciones verbales y escritas en representación de MUFACE.
- **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.

6 Provisión del servicio

La provisión tanto para dispositivos corporativos como para dispositivos no corporativos se formalizará con la firma de un documento de aceptación por parte de los usuarios, similar al del Anexo II Modelo de Documento de Aceptación.

Se podrán establecer límites y controles en el servicio de voz y datos como por ejemplo limitar el ancho de banda, tarifas aplicadas, servicios de roaming permitidos, etc.

Toda información de nivel alto de confidencialidad deberá estar cifrada en el dispositivo.

Es obligatorio restringir el acceso del dispositivo mediante mecanismos de bloqueo (como por ejemplo contraseña con pin de 6 dígitos, contraseña alfanumérica, patrón de desbloqueo, uso de biometría, etc.).

Si existe la posibilidad, se habilitará el borrado remoto de los datos del dispositivo corporativo y configuraciones del dispositivo, y en caso de robo o pérdida, se deberá proceder al borrado remoto de la información corporativa.

6.1 Recursos corporativos

MUFACE, en seguimiento de sus políticas de asignación de recursos, pone a disposición de los usuarios los recursos de movilidad necesarios para el cumplimiento de sus obligaciones. En consecuencia, dichos recursos de movilidad corporativos (hardware, software y acceso a las comunicaciones móviles) no está destinado al uso personal o extra-profesional de los usuarios, los cuales deben conocer que no gozan de un uso privativo del mismo. Deberá tenerse en cuenta que los recursos asignados podrán ser a veces compartidos con otros usuarios (números de línea, dispositivos móviles, módems, etc.).

Se solicitará la asignación de recursos de movilidad corporativos a las Unidades TIC correspondientes según el procedimiento específico definido para ello. Éstas evaluarán la petición y podrán proporcionarlo o denegarlo en función de la disponibilidad de recursos y los criterios de asignación establecidos.

Se llevará un inventario de los recursos móviles asignados junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

El área TIC de MUFACE junto con las unidades TIC de la AEAD, serán las responsables de configurar los dispositivos móviles corporativos, definir las aplicaciones de uso corporativo y proceder a su instalación, configuración y desinstalación. El software instalado cumplirá con las condiciones de licenciamiento o uso exigibles legalmente y se configurará teniendo en cuenta el principio básico de seguridad por defecto del Esquema Nacional de Seguridad (ENS).

Como parte de la instalación y configuración de los dispositivos, se podrá instalar y configurar software de seguridad y de gestión remota. El objeto de este software será proteger la seguridad de la información de MUFACE y, al mismo tiempo, preservar la privacidad y la intimidad del usuario del dispositivo. Para ello se podrá establecer un

procedimiento de plataformado o configuración de dispositivos de movilidad de MUFACE, y las instrucciones de manejo se indicarán al usuario a la recepción del dispositivo.

Los dispositivos móviles tendrán configurado un bloqueo de pantalla automático por inactividad que se activará de manera automática después del tiempo máximo de inactividad definido en la norma o política específica de cada ámbito, que será de 5 minutos en el caso de no estar especificado en dicha norma, solicitando la introducción de la contraseña de usuario.

Toda instalación, desinstalación o cambio de configuración de software o hardware en el equipamiento de MUFACE deberá ser realizada o autorizada previamente por la Unidad TIC y consultado con el área o unidad correspondiente de la AEAD.

Se informará a cada usuario de los deberes, responsabilidades y recomendaciones en el uso de los recursos de movilidad de MUFACE, poniendo a su disposición la información en su intranet.

Al finalizar la relación de servicio con MUFACE por parte de un usuario, deberá devolver el equipamiento que le fue asignado. Asimismo, si en algún momento deja de darse cualquier otra circunstancia que, según los criterios de MUFACE, constituye un requisito necesario para la asignación de un recurso de movilidad deberá procederse a su devolución.

La Unidad TIC se encargará de enviar el dispositivo a la AEAD para proceder con el borrado seguro de la información previamente a su reutilización o desafectación. Se entiende por borrado seguro aquel que garantiza que no se pueda recuperar información que ha sido eliminada del sistema.

6.2 Recursos no corporativos

El uso de recursos no corporativos para fines corporativos deberá estar previamente autorizado y supervisado por MUFACE para garantizar que no se ponga en peligro la seguridad de la información de muface ni la privacidad e intimidad del usuario.

Para ello, es necesario el consentimiento expreso del propietario del recurso para usar su dispositivo o línea no corporativa para un uso corporativo.

La gestión y administración de los dispositivos y recursos no corporativos correrá a cargo del propietario. MUFACE no tiene ni contrae ningún tipo de obligación para con los recursos no corporativos.

MUFACE se reserva el derecho de requerir la instalación del software y salvaguardas que estime oportuno para garantizar las condiciones de seguridad. Para ello se podrá establecer un procedimiento de habilitación de dispositivos personales.

El conjunto de medidas de seguridad requeridas podrá incluir:

- Validación del dispositivo previa al acceso a recursos de MUFACE.
- Cifrado de la información residente en el dispositivo.
- Medidas de prevención de usos prohibidos del dispositivo.
- Instalación y configuración de recursos corporativos.
- Localización y borrado remoto de los datos del dispositivo en caso de que el dispositivo haya sido extraviado o robado.

MUFACE determinará los dispositivos con su correspondiente versión de sistema operativo que están permitidos, así como el inventario de los dispositivos autorizados.

Se podrá establecer un procedimiento de finalización del uso corporativo de un dispositivo no corporativo, que consistirá en la eliminación segura de las aplicaciones e información corporativa, así como del software de control y de acceso. En caso necesario MUFACE podrá solicitar o efectuar si tuviese control sobre el dispositivo, el borrado del dispositivo o la restauración a valores de fábrica.

7 Normas de uso

Se informará a cada persona que tenga acceso a los sistemas, de los deberes y responsabilidades en el uso de los recursos de movilidad de MUFACE.

Se especificarán las medidas disciplinarias a que haya lugar.

Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.

Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

7.1 Usos autorizados

En general son usos autorizados de los recursos de movilidad aquellos que no comprometen la seguridad de la información de MUFACE ni la privacidad e intimidad de sus usuarios, y que se ajusten al propósito por el cual fueron asignados.

El uso de los recursos de movilidad corporativos es para asuntos relacionados con el desempeño de las funciones que correspondan al puesto de trabajo del usuario.

Los usuarios se limitarán a trabajar con los recursos móviles que le han sido asignados (recursos corporativos) o cuyo uso ha sido previamente autorizado (recursos no corporativos), y en caso de requerir más recursos deberán solicitarlos a través de los canales establecidos a tal efecto.

Los dispositivos móviles corporativos serán manipulados, únicamente por personal técnico autorizado.

El software corporativo se utilizará siguiendo las normas, instrucciones o indicaciones de uso emitidas por la Unidad TIC correspondiente.

El acceso desde los dispositivos móviles a la red corporativa se realizará atendiendo a la norma de transmisión de la información.

7.2 Usos no autorizados

Se prohíbe todo uso de recursos de movilidad que pongan en riesgo la seguridad de la información de MUFACE o la privacidad o la intimidad de sus usuarios.

Son usos no autorizados:

7.2.1. Manipulación no autorizada de los recursos de movilidad:

- Emplear los recursos de movilidad sin una autorización formal por parte de la Unidad TIC.

- Manipular los equipos corporativos 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 dispositivos, salvo el personal técnico autorizado.
- Manipular los dispositivos móviles corporativos en situaciones de riesgo por contacto con líquidos, exposición a la lluvia, caídas desde alturas, cerca de alimentos y bebidas, etc., que puedan originar directa o indirectamente su mal funcionamiento.
- Acciones que conlleven la pérdida de la garantía del recurso corporativo.
- Modificar la configuración para acceder al sistema operativo a bajo nivel, alterando las medidas de seguridad impuestas por los fabricantes ("jailbreak" en dispositivos IOS, "rooteado" en dispositivos Android, etc.).
- 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.

7.2.2. Conexión con redes públicas no seguras

- Está expresamente prohibida la conexión/ habilitación de dispositivos móviles que faciliten la transferencia de información de manera inalámbrica que no reúna los requisitos de seguridad mínimos que garanticen la confidencialidad de la información (WIFI, Bluetooth, o infrarrojos).
- Permitir conexiones desde el exterior a los dispositivos móviles corporativos mediante mecanismos no autorizados por el Responsable de Seguridad correspondiente.
- Conectar los dispositivos móviles a redes no securizadas atendiendo a lo establecido en la norma de transmisión de la información.

7.2.3. Almacenamiento de información y configuración no autorizados

- No está permitido almacenar información sensible o confidencial, salvo autorización del responsable de dicha información.
- Instalar en los dispositivos móviles corporativos 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.

- Desinstalar software, borrar archivos del sistema, o cambiar configuraciones de los dispositivos móviles corporativos y programas sin la autorización y supervisión de la Unidad TIC.
- Desactivar el software antivirus o sus actualizaciones, o cualquier mecanismo de seguridad instalado en el equipo.
- 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.
- El uso de aplicaciones que permitan la compartición de información corporativa sin cifrar de forma incontrolada (aplicaciones de compartición de documentos p2p o en la nube).
- Uso del equipamiento corporativo con fines comerciales o de obtención de lucro económico.
- Sincronizar la información confidencial con alguna aplicación externa no autorizada por MUFACE.
- No respetar la legislación de derechos de autor y propiedad intelectual en el software o material en formato electrónico utilizado en los equipos. Enviar mensajes con información confidencial a destinatarios no autorizados, con especial atención a los envíos al exterior de MUFACE.
- Enviar sin autorización mensajes de forma masiva.
- No se podrá usar las líneas de MUFACE para servicios Premium de mensajería.
- Realizar acciones tales como ejecutar software, abrir o reproducir cualquier tipo de ficheros (documentos, imágenes, contenidos multimedia, etc.) o enviar mensajes que puedan ser constitutivos de delito. Si los comportamientos pudieran ser considerados como actos delictivos tipificados, se procedería a realizar el correspondiente traslado al Ministerio Fiscal.
- Incumplir cualquier otra norma, instrucción o procedimiento relacionado con el uso del equipamiento software y hardware emitida por MUFACE.
- 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.

8 Recomendaciones de uso

La movilidad conlleva unos riesgos asociados a la posibilidad de pérdida o robo del dispositivo, produciéndose una pérdida de confidencialidad de la información contenida en el mismo.

A continuación, se enumerarán las medidas disponibles que se pueden llevar a cabo para incrementar la seguridad en los dispositivos móviles. Sin perjuicio de las recomendaciones de uso que publique MUFACE en su intranet o que algunas de ellas sean requeridas por MUFACE para el uso corporativo de los dispositivos:

- Cifrado de la memoria: Se recomienda cifrar la memoria de almacenamiento. De esta forma se dificultaría la copia o extracción de datos si no se conoce la contraseña de desbloqueo.
- Se recomienda disponer de un antivirus en el dispositivo móvil como medida extra de protección.
- Anotar el IMEI (Identidad Internacional de Equipo Móvil) del dispositivo y almacenarlo en un lugar seguro.

Para los dispositivos no corporativos, algunas de las recomendaciones adicionales son:

- El principal problema de infecciones en dispositivos móviles no corporativos es por causa de la instalación de programas desde fuentes desconocidas. Es muy importante instalar aplicaciones únicamente desde los repositorios oficiales del dispositivo.
- Se desaconseja conceder privilegios de administrador a las aplicaciones.
- Es recomendable desinstalar toda aplicación que no sea estrictamente necesaria para el desempeño del dispositivo, y así minimizar el riesgo de exposición por una aplicación vulnerable.
- Siempre que el sistema notifique de una actualización disponible, se debe aceptar y aplicar la nueva versión. Manteniendo el sistema actualizado se evitan posibles infecciones por aplicaciones vulnerables.

9 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 las Unidades TIC 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 memorias SD, limitación de conexiones de red, Wifi, 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 corporativos 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 recurso de movilidad a los usuarios involucrados, la suspensión del servicio o inhabilitación del recurso, así como exigir la inmediata devolución de estos.

10 Reporte de incidentes de seguridad

El usuario deberá reportar cualquier incidente que considere relevante y que pueda afectar a la seguridad, 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 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 los dispositivos móviles deberá comunicarse de manera inmediata. En el caso de sustracción dicha comunicación deberá acompañarse con la correspondiente denuncia policial.

11 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.

12 Responsabilidades

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte del personal de MUFACE 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.

Los usuarios son responsables de la custodia de los recursos móviles, así como de la información almacenada en ellos. Por tanto, son responsables de la integridad y de la copia de seguridad de la información de sus dispositivos móviles. La Unidad TIC correspondiente de la AEAD facilitará el soporte técnico necesario para completar las actuaciones de Backup y Recuperación que el usuario solicite en los dispositivos corporativos.

Los usuarios son responsables de cualquier actuación irregular o no autorizada realizada desde los recursos móviles que tienen asignados.

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.

13 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.
- CSIRT-CV. Guía de buenas prácticas en el uso corporativo de dispositivos móviles.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-450: Seguridad en dispositivos móviles

Las directrices estipuladas en esta norma se fundamentan en los requisitos establecidos en el ENS que se mencionan a continuación[1].

13.1 Medida mp.eq.3 – Protección equipos portátiles

Categoría MEDIA

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.

[1] Se trata de una extracción de aspectos o medidas específicos del ENS (Real Decreto 311/2022) en relación con lo tratado en esta norma, con el fin de que el presente documento sea auto contenido y de más fácil lectura.

- 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.

13.2 Medida mp.si.2 - Criptografía

Categoría MEDIA

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.

13.3 Medida mp.si.3 - Custodia

Categoría MEDIA

- 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.

13.4 Medida mp.si.5 – Borrado y destrucción

Nivel MEDIO

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].

13.5 Medida mp.info.1 – Datos de carácter personal

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

13.6 Medida mp.info.3 – Protección de dispositivos portátiles

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.

13.7 Medida mp.info.6 – Copias de seguridad

Nivel MEDIO

- 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.

14 Anexo II: Modelo de documento de aceptación

D/Dª (nombre del trabajador/a) con DNI nº (número de DNI), empleado de (nombre de la empresa), declaro haber sido pertinentemente informado de la política de uso de los recursos móviles de MUFACE.

Este compromiso implica:

- *La observancia de las medidas de uso responsable especificadas por MUFACE.*
- *El compromiso de evitar situaciones de riesgo para la seguridad de la información de MUFACE.*
- *Cumplimiento de los requisitos técnicos especificados por MUFACE.*
- *Aceptación de la supervisión de MUFACE tal y como está reflejado en la norma de uso y provisión de dispositivos móviles*

Declaro, asimismo, haber recibido las instrucciones precisas para el efectivo cumplimiento de las obligaciones que asumo respecto al uso de recursos de movilidad. Mi compromiso en los términos del presente acuerdo se extenderá durante el periodo que preste servicios para MUFACE, cumpliendo con los requisitos de finalización de la relación definidos por MUFACE.

El cumplimiento de estos compromisos perdurará incluso una vez finalizada mi relación profesional con MUFACE.

Lugar y Fecha Firma del empleado