NORMA DE DEBERES Y OBLIGACIONES DEL RESPONSABLE DEL PUESTO DE TRABAJO

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

Contenido

1. OBJETO 3

2. ÁMBITO DE APLICACIÓN 4

3 CONTEXTO DE LA PRESENTE NORMA 4

4 VIGENCIA 5

5 TERMINOLOGÍA RELEVANTE 5

6 RESPONSABILIDAD EN MATERIA DE SEGURIDAD 6

7 FUNCIONES Y OBLIGACIONES DEL PERSONAL 7

7.1 Aspectos generales 7

7.2 Confidencialidad de la Información 8

7.3 Perfiles con características especiales 9

7.3.1 Administrador 9

7.3.2 Operador 9

8 FORMACIÓN Y CONCIENCIACIÓN 10

9 REPORTE DE INCIDENTES DE SEGURIDAD 11

10 REVISIÓN DE LA NORMA 11

11 RESPONSABILIDADES 11

12 ANEXO I: REFERENCIAS 12

12.1 Medida mp.per.1 12

12.2 Medida mp.per.2 12

12.3 Medida mp.per.3 13

12.4 Medida mp.per.4 13

12.5 Medida mp.eq.1 14

12.6 Medida mp.eq.2 14

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. Objeto

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.

El objeto de este documento es abordar la problemática que surge en relación con los elementos humanos que intervienen en el proceso, así como a sus responsables jerárquicos, para que "...ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad".

La Norma de Organización de la Seguridad y Responsabilidades, es dónde se definen las responsabilidades en materia de seguridad de los diversos roles relacionados con la seguridad que existen dentro de la organización y la Norma de Deberes y Obligaciones del Personal y Empresas Externas, complementan la presente norma.

El objeto de esta norma es aplicable en materia de seguridad a las funciones y obligaciones del personal, estableciendo los requisitos y medidas que deben ser adoptadas para garantizar la protección de los sistemas de información de MUFACE.

2. Ámbito de aplicación

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

3 Contexto de la presente norma

La presente norma se integra 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 establecidos en el Anexo II de las medidas de seguridad mp.per.1 - Caracterización del puesto de trabajo, mp.per.2 - Deberes y obligaciones, mp.per.3 – Concienciación, mp.per.4 – Formación, mp.eq.1 – Puesto de trabajo despejado, mp.eq.2 – Bloqueo de puesto de trabajo, del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

Establece las directrices que se deben observar en relación a la definición y asignación de los puestos de trabajo, así como las responsabilidades correspondientes, formación y concienciación en materia de seguridad para el personal de la SEAP.

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 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 correspondiente 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.

- **Responsables de la Información**: según define la PSI, la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a la seguridad. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestiones el procedimiento o trámite.
- **Responsables del Servicio**: según define la PSI, la persona que determina los requisitos de seguridad de los servicios prestados. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa de cada servicio.
- **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 Responsabilidad en materia de seguridad

La Norma de Organización de la Seguridad y Responsabilidades define las responsabilidades en materia de seguridad de los diversos roles relacionados con la seguridad existente en la organización, así como la estructura organizativa de la seguridad, es decir, los diversos comités y grupos técnicos que acuerdan y aprueban la normativa de seguridad y velan por su cumplimiento y adecuación al ENS.

La estructura organizativa de la gestión de la seguridad en MUFACE se articula según los Comités, Oficina y los Roles de seguridad existentes en MUFACE y que se detallan a continuación:

- Comité de Seguridad de la Información.
- Oficina de Seguridad de la Información.
- Responsables del Servicio.
- Responsables del Sistema.
- Responsables de la Información.
- Responsables de Seguridad.

7 Funciones y obligaciones del Personal

Se informará a cada persona que tenga acceso a los sistemas, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

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.

En caso de personal contratado a través de un tercero, se tomará como referencia la Norma de Deberes y Obligaciones del Personal y Empresas Externas.

7.1 Aspectos generales

Todo el personal de MUFACE con acceso a los sistemas de información debe garantizar el cumplimiento de las directrices establecidas en las distintas normas de uso seguro de los sistemas, que forman parte del desarrollo normativo de seguridad derivado de la Política de Seguridad de la Información.

Los puestos de trabajo deberán permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

Así mismo, el material de trabajo se guardará en lugar cerrado cuando no se esté utilizando, cuando el nivel de seguridad de la información así lo precise.

El usuario deberá bloquear por contraseña su puesto de trabajo en el caso que se ausente del mismo de manera temporal.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información se deberán adecuar a lo dispuesto en la normativa aplicable en materia de protección de datos (RGPD y LOPDGDD).

Se debe suministrar al personal que maneje datos de carácter personal u otra información cuya protección sea necesaria, el mobiliario adecuado para guardar la información (en soporte papel o electrónico).

En particular, se tendrán en cuenta las siguientes directrices:

- Utilizar contraseñas fuertes en todos los servicios, para dificultar la suplantación de identidad (evitar nombres, fechas, datos conocidos o deducibles, etc.).
- Nunca utilizará la misma contraseña para más de una cuenta.
- Bajo ninguna circunstancia deberá compartir su contraseña con un desconocido.
- No escribirá físicamente tu contraseña en ningún lugar donde podría ser descubierto fácilmente por otras personas.
- Existirá un procedimiento de gestión de contraseñas.
- Para evitar virus, deberá descargar los ficheros sólo de fuentes confiables.
- Analizar con un antivirus todo lo que se descargue antes de ejecutarlo.

7.2 Confidencialidad de la Información

Con objeto de garantizar la confidencialidad de la información a la que el usuario pueda tener acceso en el ejercicio de sus funciones, se deberán observar las siguientes directrices:

- Mantener el secreto profesional respecto a la información confidencial a la que el usuario pueda tener acceso en el ejercicio de sus funciones. Esta obligación persistirá por tiempo indefinido, incluso después de finalizar sus relaciones MUFACE.
- Garantizar la realización de un tratamiento adecuado de la información, evitando cualquier modificación, alteración o destrucción de la misma.
- Reducir el uso de información confidencial a lo estrictamente necesario, adoptando las precauciones y medidas necesarias para evitar el acceso a esta información a personas no autorizadas.
- Guardar todos los soportes físicos que contengan información confidencial en un lugar seguro, con acceso limitado a las personas debidamente autorizadas.

- No enviar nunca información confidencial a terceros, por cualquier medio (en soporte papel, magnético, electrónico, etc.), a no ser que se disponga de autorización para hacerlo.
- No permitir nunca el acceso a datos por parte de terceros si esta relación no se ajusta a lo establecido en los Contratos de Prestación de Servicios establecidos al efecto.

7.3 Perfiles con características especiales

Los diferentes perfiles del personal de MUFACE con acceso a los sistemas de información deberán cumplir con las directrices establecidas en las distintas normas de uso seguro de los sistemas, que forman parte del desarrollo normativo de seguridad derivado de la Política de Seguridad de la Información.

Entre otros perfiles están:

7.3.1 Administrador

Las tareas de un Administrador en materia de seguridad entre otras son:

- Crear diferentes usuarios, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas. Para aumentar la seguridad, se crearán usuarios con el nivel de privilegio adecuado para las tareas que deban realizar.
- Controlar y reducir al mínimo el número de usuarios con nombres y contraseñas de administrador. Se accederá al sistema con el nivel de privilegio mínimo para cada tarea.
- Deben controlar los puertos abiertos de la red, y bloquear los que no se utilicen.
- Descargar archivos sólo de sitios de confianza.
- Responsabilidad en las copias de respaldo.

7.3.2 Operador

Un operador en materia de seguridad entre otras tareas deberá:

- Gestionar alertas.
- Resolver incidencias.

- Controlar y monitorizar los sistemas y las comunicaciones.

8 Formación y Concienciación

Se formará al personal en aquellas materias de seguridad que requieran para el desempeño de sus funciones, en particular en lo relativo a configuración de sistemas, detección y reacción a incidentes y gestión de la información en cualquier soporte en el que se encuentre, de acuerdo con las necesidades de formación en materia de seguridad de cada puesto de trabajo, de las carencias del personal que lo ocupa y de los cursos de formación disponibles en cada momento.

Se debe disponer de un Plan de Formación para los puestos de trabajo que desempeñen actividades específicas de seguridad.

Se deberá garantizar que el usuario, que en el desempeño de sus funciones trate con datos de carácter personal, esté sensibilizado respecto de los riesgos que puede implicar un tratamiento incorrecto de esta información.

Como parte de las obligaciones del Responsable de Seguridad se realizará las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidades.

Se debe disponer de un Plan de Concienciación que debe ser desplegado en todos los niveles de la Secretaría de Estado que establezca el diseño de medios de comunicación y difusión adecuados para el despliegue de campañas de concienciación en materia de seguridad.

Se recordará regularmente:

- La normativa de seguridad relativa al buen uso de los sistemas.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento de reporte de incidencias de seguridad.

9 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.

10 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.

11 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.

Las responsabilidades asociadas a cada componente de la estructura organizativa para la gestión de la seguridad en MUFACE es la definida en la Norma de Organización de Seguridad y Responsabilidades.

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.

12 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[1].

12.1 Medida mp.per.1

Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.

Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

12.2 Medida mp.per.2

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

- Las medidas disciplinarias a que haya lugar.

[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.

- Contemplando 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.
- El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
- En caso de personal contratado a través de un tercero:
    - Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
    - Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

- Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

12.3 Medida mp.per.3

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

- La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

12.4 Medida mp.per.4

Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.

c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

12.5 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.

12.6 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.