NORMA DE DEBERES Y OBLIGACIONES DEL PERSONAL Y EMPRESAS EXTERNAS

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información (Marco Organizativo)

Versión del documento 1.0

INDICE

INTRODUCCIÓN **4**

2 ÁMBITO DE APLICACIÓN **4**

3 CONTEXTO DE LA PRESENTE NORMA **4**

4 VIGENCIA **5**

5 DEBERES Y OBLIGACIONES DE LAS EMPRESAS SUMINISTRADORAS **5**

6 DEBERES Y OBLIGACIONES DEL PERSONAL EXTERNO **6**

7 DEBERES Y OBLIGACIONES DEL PERSONAL INTERNO CON RESPONSABILIDAD EN LA DIRECCIÓN DE PROYECTOS EJECUTADOS POR PERSONAL O EMPRESAS EXTERNAS **7**

8 RESPONSABILIDADES **7**

9 REVISIÓN DE LA NORMA **8**

10 ANEXO III: CLÁUSULA SOBRE CONFIDENCIALIDAD **8**

10.1 Modelo de acuerdo de confidencialidad 8

11 ANEXO V: REFERENCIAS **8**

11.1 Artículo 6 del ENS: La seguridad como un proceso integral. 9

11.2 Medida mp.per.2 10

11.3 Medida op.acc.4 10

11.4 Medida op.ext.1 11

11.5 Medida op.ext.2 11

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

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 su artículo 6, el ENS otorga especial importancia a la concienciación de las personas que intervienen en el proceso, así como, de 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.

En este contexto se hace necesario definir las directrices que marquen las pautas de comportamiento y los deberes y obligaciones del personal externo que presta sus servicios para MUFACE, así como, los de las personas responsables de su control y seguimiento, de manera que quede garantizada la seguridad en los sistemas y servicios.

2 Ámbito de aplicación

Esta norma aplica a todas las empresas que puedan ser suministradoras de productos o servicios destinados a MUFACE, así como, al personal externo que realiza sus funciones para MUFACE, bien sea en sus instalaciones o fuera de ellas.

Es también de aplicación para las personas con responsabilidad en la gestión y dirección de proyectos ejecutados por personal o empresas externas.

3 Contexto de la presente norma

Este documento forma parte del cuerpo normativo de la Política de Seguridad de la Información (PSI) de MUFACE, desarrollado para garantizar la seguridad de la información en la misma.

El *Responsable de Seguridad* correspondiente 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 Deberes y obligaciones de las empresas suministradoras

Las empresas suministradoras de componentes y servicios se comprometerán a cumplir lo indicado en las cláusulas relacionadas con el cumplimiento de las medidas de seguridad expresadas en la Norma de gestión de suministradores.

En el caso de que se permita subcontratación de terceros, y se lleve a cabo, la empresa que ha firmado el contrato con la Administración velará porque la empresa subcontratada cumpla con los requisitos y medidas de seguridad requeridos y expresados en el Pliego de Prescripciones Técnicas y, en general, velará porque se cumplan aquellas medidas de seguridad requeridas por el Esquema Nacional de Seguridad y por la Normativa de Protección de Datos Personales en el caso de que se realice un tratamiento de datos personales.
Existirá una figura de responsable de seguridad por parte del proveedor que será el interlocutor en materia de seguridad con el responsable de seguridad designado por MUFACE para el ámbito que contrata.

La empresa suministradora del desarrollo de sistemas de información se comprometerá al cumplimiento de lo indicado en la Norma de gestión de la seguridad en el ciclo de vida de los sistemas de información.

En todo caso, pero en especial cuando se lleva a cabo el desarrollo de servicios en instalaciones ajenas a MUFACE, estará obligada a la notificación de los incidentes de seguridad que puedan haberse producido, facilitando la recolección de evidencias y el seguimiento y la pronta resolución de los mismos.

Se evitará en lo posible los accesos remotos a las instalaciones donde se estén prestando los servicios. En el caso de que sea imprescindible, se realizarán con las debidas medidas de seguridad según lo indicado en la *Norma de trasmisión de la información*.

Deberá disponer de un plan de continuidad que permita recuperar la información en caso de desastres y que tenga previstos medios alternativos que permitan continuar con la actividad en caso de contingencias. Esto incluirá el reemplazo del personal dedicado a prestar los servicios en el tiempo indicado en el acuerdo de nivel de servicios en el caso de indisponibilidad del mismo.

La empresa suministradora de servicios proporcionará formación en seguridad al personal involucrado en la prestación de los mismos. Deberán conocer las medidas de seguridad exigibles por el Esquema Nacional de Seguridad y por las guías CCN-STIC, así como, todas aquellas normas y procedimientos de seguridad de MUFACE que sean de aplicación en su puesto de trabajo.

En el caso de prestación de servicios en instalaciones ajenas a MUFACE, la empresa suministradora proporcionará un listado de los usuarios con acceso a los sistemas de información, con indicación de los perfiles asignados a cada uno de ellos. Los privilegios asignados a estos perfiles se basarán en los principios de mínimo privilegio y necesidad de conocer, según lo indicado en la medida op.acc.4 del ENS. El responsable de seguridad asignado al proyecto por la empresa suministradora velará por la adecuada gestión de dichos derechos de acceso.

6 Deberes y obligaciones del personal externo

El personal externo tendrá la obligación de conocer y cumplir lo indicado en las Normas de seguridad de MUFACE.

Le será de aplicación en especial lo indicado en la Norma de Deberes y Obligaciones del Responsable del Puesto de Trabajo.

Deberá firmar un Acuerdo de Confidencialidad de manera previa a su incorporación al puesto de trabajo.

7 Deberes y obligaciones del personal interno con responsabilidad en la dirección de proyectos ejecutados por personal o empresas externas

Las personas con responsabilidad en la dirección de proyectos ejecutados por empresas externas se asegurarán del cumplimiento por parte de éstas de las medidas de seguridad requeridas.

De igual manera, realizarán un seguimiento del cumplimiento de las pautas de seguridad del personal externo que lleve a cabo sus funciones bajo su dirección en las instalaciones de MUFACE.

Se asegurarán, entre otros temas, de la firma de los correspondientes acuerdos de confidencialidad por parte del personal externo bajo su dirección de manera previa a su incorporación a los proyectos.

Ajustarán los permisos asignados a los usuarios utilizados por el personal externo a los estrictamente necesarios para el cumplimiento de su función, y procederán a solicitar la desactivación de dichos usuarios cuando finalice su intervención en los proyectos.

Gestionará los incumplimientos de obligaciones por parte de las empresas o personal externo según lo indicado en el correspondiente procedimiento de resolución de incumplimientos.

8 Responsabilidades

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte de las personas con responsabilidad en la gestión de la seguridad en MUFACE así como por aquellos con responsabilidad en la adquisición de componentes y servicios y en el seguimiento del cumplimiento de los requisitos especificados, 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 la SEAP 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.

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 Anexo III: Cláusula sobre confidencialidad

10.1 Modelo de acuerdo de confidencialidad

Podrá utilizarse como referencia lo indicado en la guía CCN-STIC-821: Esquema Nacional de Seguridad. Normas de seguridad, en su apéndice VI: Acuerdo de confidencialidad para terceros.

11 Anexo V: 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.
- Política de Seguridad de MUFACE.

- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-205: Actividades de seguridad en el ciclo de vida de los sistemas TIC.
- 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.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-819: Esquema Nacional de Seguridad. Contratación en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-821: Esquema Nacional de Seguridad. Normas de seguridad.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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

11.1 Artículo 6 del ENS: La seguridad como un proceso integral.

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los 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.

[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.

11.2 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.
- 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.

11.3 Medida op.acc.4

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- Todo acceso estará prohibido, salvo autorización expresa.
- Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
- Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.

- Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
- Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

11.4 Medida op.ext.1

Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos

11.5 Medida op.ext.2

Se establecerá lo siguiente:

- Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
- El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).