Política de Seguridad de la Información

MUFACE

Documentación: MUFACE -Seguridad

UNIDAD INFORMÁTICA

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información (Marco Organizativo)

Versión del documento 1.3

Ministerio para la Transformación Digital
y de la Función Pública

INDICE

1 APROBACIÓN Y ENTRADA EN VIGOR 5

2 INTRODUCCIÓN 5

3 ALCANCE 6

4 MISIÓN 6

5 MARCO NORMATIVO 7

6 PRINCIPIOS BÁSICOS 7

7 ORGANIZACIÓN DE LA SEGURIDAD 9

7.1 Definición de Roles de Seguridad 9

7.2 Proceso de toma de decisiones y coordinación 10

7.3 Proceso de designación y Resolución de Conflictos 11

7.4 Detalle de los Roles 11

7.4.1 Dirección (Consejo de Dirección) 11

7.4.2 Comité de Seguridad 12

7.4.3 Responsable de Seguridad 14

7.4.3.1 Responsables de Seguridad Delegados 15

7.4.4 Responsable del Servicio y de la Información 16

7.4.5 Responsable del Sistema 17

7.4.6 Delegado de Protección de Datos (DPD) 18

8 DATOS DE CARÁCTER PERSONAL 18

9 ANÁLISIS Y GESTIÓN DE RIESGOS. 19

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 20

10.1 Instrumentos de Desarrollo y Gestión de la Documentación 20

10.2 Estructura General 21

10.3 Gestión de la documentación 21

10.4 Sanciones previstas por incumplimiento 23

11 SEGURIDAD DE LA INFORMACIÓN 23

11.1 Calificación de la Información 23

12 OBLIGACIONES DEL PERSONAL 24

13 TERCERAS PARTES 25

13.1 Terceras Partes como Servicios Externalizados de Seguridad 26

14 DESARROLLO DEL SGSI, REVISIÓN Y AUDITORIAS 26

ANEXO 1. ACRÓNIMOS 28

Cuadro Resumen del Documento

Titulo	PSI Política de Seguridad de la Información de MUFACE
Referencia	Oficina de Seguridad de la Información (Unidad Informática)
Autor	Babel Sistemas de Información
Fecha de elaboración	Septiembre de 2024

Control de Cambios

Revisado por	Aprobado por	Fecha
Leonardo González	Comité de Seguridad	30/07/2025

Control de Cambios

Versión	Fecha	Autor	Descripción de la modificación
1.0	21/08/2024	Babel Sistemas	Versión inicial
1.1	12/09/2024	Babel Sistemas	Revisión
1.2	19/09/2024	Babel Sistemas	Revisión
1.3	24/09/2024	Babel Sistemas	Revisión

1 Aprobación y entrada en vigor

Esta política fue aprobada a día 30 de Julio de 2025 por el Comité de Seguridad de la Información de MUFACE, siendo ésta la última revisión a fecha de publicación (12/11/2025), y siendo efectiva desde esta fecha y hasta que sea reemplazada por una nueva.

El Comité de Seguridad de la Información de MUFACE, se compromete a difundirla y a revisarla periódicamente con la finalidad de introducir los cambios que sean convenientes.

2 Introducción

La Mutualidad General de Funcionarios Civiles del Estado (MUFACE) es un organismo público encargado de prestar asistencia sanitaria y social al colectivo de funcionarios adscritos. Se crea por la Ley 29/1975, de 27 de junio, sobre Seguridad Social de los Funcionarios Civiles del Estado, con la finalidad de gestionar el sistema de Mutualismo Administrativo de los funcionarios civiles del Estado.

MUFACE gestiona un importante conjunto de prestaciones para la protección de su colectivo, formado por 1.500.000 personas aproximadamente. A grandes rasgos, podemos distinguir:

- La asistencia sanitaria y la farmacéutica, complementaria de la anterior.
- Las prestaciones sociales que incluyen, entre otras, el subsidio por incapacidad temporal o por riesgo durante el embarazo o durante la lactancia natural, las indemnizaciones por lesiones permanentes no invalidantes o la prestación económica por gran invalidez.

Para lograr una gestión eficaz y eficiente de las mismas, MUFACE se apoya en sus sistemas de tecnologías de la información y las comunicaciones (STIC).

Estos sistemas se convierten en pilares básicos para su funcionamiento, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos definidos en el RD 311/2022 Esquema Nacional de Seguridad (en adelante, ENS).

La Política de Seguridad de la Información, que se plasma en este documento, recoge la forma en que MUFACE gestiona y protege la información y los servicios. En concreto,

aquellos que hace uso el ciudadano por medios electrónicos para el ejercicio de derechos y el cumplimiento de deberes en su relación con MUFACE.

El objetivo de la seguridad de la información es garantizar la calidad de la misma y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los STIC deben estar protegidos contra amenazas, de rápida evolución, con potencial para incidir en la integridad, disponibilidad, autenticidad, trazabilidad, confidencialidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la continuidad de los servicios prestados.

Esto implica que los diferentes departamentos en que se articula MUFACE deben cerciorarse de que la seguridad de los STIC es una parte integral de cada etapa de sus actividades y, desde su concepción hasta la retirada de servicio, deben aplicar las medidas mínimas de seguridad exigidas por el ENS para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

3 Alcance

Esta política aplica y será de obligado cumplimiento para todos los departamentos de MUFACE, así como para terceras partes con las que MUFACE comparta información o reciba algún servicio que implique el acceso a la misma.

Para facilitar su conocimiento y cumplimiento, estará disponible en el sitio web de MUFACE, así como en la intranet corporativa.

4 Misión

Asegurar al colectivo de mutualistas el acceso a las prestaciones sanitarias y farmacéuticas en las mismas condiciones que el resto del Sistema Nacional de Salud, así como facilitarles un amplio abanico de prestaciones sociales y económicas, con la

finalidad de satisfacer sus necesidades, contando con un equipo humano de calidad en la atención al público, como seña de identidad.

5 Marco Normativo

Serán de aplicación aquellas normas que regulan las actividades de MUFACE, en el ámbito de sus competencias y aquellas dirigidas a garantizar la seguridad de la información, los datos de naturaleza personal, los recursos y medios electrónicos gestionados por la Organización.

6 Principios Básicos

Todos los servicios deben estar preparados para cumplir con sus objetivos utilizando sistemas de información, por lo que deben asegurar que se cumplen los siguientes principios básicos:

1. **Seguridad Integral y Mínimos Privilegio**

MUFACE formará e informará a todo su personal acerca de los deberes y obligaciones en materia de seguridad y garantizará que la atención, revisión y auditoría de los sistemas de seguridad se lleven a cabo por personal cualificado, bajo criterios de profesionalidad, exigiendo además que las organizaciones que le presten servicios cuenten con profesionales y técnicos cualificados y con niveles idóneos de calidad y excelencia en la prestación de sus servicios.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto.

2. **Gestión de la Seguridad basada en los riesgos**

La gestión de los riesgos es parte fundamental para el proceso de seguridad. MUFACE, a través de los responsables en materia de seguridad, deberá implementar mecanismos de gestión del riesgo, minimizándolos hasta niveles aceptables mediante el despliegue de medidas de seguridad, en todo caso garantizando el equilibrio entre la naturaleza de la información, los riesgos a los que se expone y las medidas de seguridad a adoptar.

3. Prevención

Todos los servicios de MUFACE deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional que sea preciso establecer tras una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

4. Detección

Dado que los servicios son vulnerables y se pueden degradar rápidamente debido a incidentes que pueden producir desde una simple desaceleración hasta su detención, se monitorizarán las operaciones de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el ENS.

5. Respuesta

MUFACE debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Establecer un punto de contacto para comunicar incidentes detectados en otros servicios o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6. Recuperación

Dentro del Plan general de continuidad de los servicios y actividades de recuperación se desarrollarán planes de continuidad de los STIC para garantizar la disponibilidad de los servicios críticos en caso de incidencia, incluyendo la copia de seguridad de los sistemas de información.

7. Existencia de líneas de defensa

MUFACE cuenta con una estrategia de protección formada por múltiples capas de seguridad que permitan reaccionar ante incidentes inevitables; reducir la probabilidad de que el sistema quede comprometido y minimizar el impacto de un incidente ya producido.

8. **Reevaluación Periódica y Vigilancia Continua**

MUFACE implementará mecanismos para la detección de actividades o comportamientos anómalos y su oportuna respuesta.

9. **Diferenciación de Responsabilidades**

A través de la presente Política de Seguridad y la normativa que la desarrolle se definirán los distintos roles intervinientes en el sistema de información.

7 Organización de la Seguridad

La gestión de la seguridad de la información implica la existencia de una estructura organizativa que, en consonancia con el ENS, defina unas responsabilidades diferenciadas en relación con los requisitos de la información, del servicio y de la seguridad.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de MUFACE, son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo con las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad de MUFACE, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

7.1 Definición de Roles de Seguridad

A continuación, se identifican los roles que participaran en la Seguridad de la Información de MUFACE:

Rol	Funciones
Comité de Seguridad de la Información	Es el órgano encargado de tomar decisiones que concretan cómo alcanzar los objetivos en materia de seguridad de la información marcados por MUFACE.

Responsable de Seguridad	Funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de los servicios.
Responsable de la Información	Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por MUFACE y en qué condiciones debe llevarse a cabo su tratamiento.
Responsable del Servicio	Tiene la responsabilidad última de determinar los niveles de servicio aceptables y la seguridad que requiere la información manejada en su Servicio o área. Determina los requisitos de seguridad de la información tratada y de los servicios prestados dentro de su Servicio o área.
Responsable del Sistema	A nivel operacional, toma decisiones operativas: arquitectura del sistema, requisitos a tener en cuenta, instalaciones y operación del día a día.
Responsables de Seguridad Delegados	Darán apoyo al Responsable de Seguridad, colabora en la elaboración y revisión de normativas y documentación, planes de mejora y campañas de concienciación (todo ello en materia de seguridad) y supervisa el estado de seguridad de los sistemas de su ámbito de responsabilidad.
Responsable del Sistema Delegado	Dará apoyo al Responsable del Sistema, implementa, ejecuta y mantiene las medidas de seguridad aplicables a los sistemas de información. (SGAD)
Delegado de Protección de Datos (DPD)	Es la persona encargada de asesorar a los responsables en materia de seguridad acerca del cumplimiento de la normativa de protección de datos personales.

7.2 Proceso de toma de decisiones y coordinación

Los diferentes roles de seguridad de la información se articularán mediante la siguiente jerarquía: el Comité de Seguridad de la Información, dará instrucciones al Responsable de la Seguridad que, junto a los Responsables de Seguridad Delegados, se encargará de supervisar que el Responsable de Sistemas y los Responsables de Sistemas Delegados implementan las medidas de seguridad según lo establecido en la Política de Seguridad de MUFACE.

7.3 Proceso de designación y Resolución de Conflictos

El Consejo de Dirección, nombrará formalmente y de conformidad con su régimen de funcionamiento interno:

- Al Responsable de la Seguridad de la Información.
- A los Miembros del Comité de Seguridad de la Información de MUFACE.

La resolución de conflictos entre los distintos roles y responsabilidades del sistema, así como las posibles incompatibilidades serán analizadas por el Comité de Seguridad, quien elevará su opinión al Consejo de Dirección para la toma de decisiones.

7.4 Detalle de los Roles

7.4.1 Dirección (Consejo de Dirección)

La función de Dirección la desempeñará el Consejo de Dirección, quien entiende la misión de la organización, determina los objetivos a alcanzar y efectúa el seguimiento de su nivel de cumplimiento.

Le corresponde:

1. Designar los diferentes roles encargados de la gestión de la seguridad, así como los miembros del Comité de Seguridad.
2. Fijar anualmente unos objetivos de nivel de riesgo aceptable. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de MUFACE, ser medibles o estimables y coherentes con las presentes directrices. El Comité de Seguridad apoyará al Consejo de Dirección en la fijación y aprobación de estos objetivos y reportará anualmente la evolución de dichos objetivos.
3. Aprobar el Plan de Adecuación al ENS.
4. Aprobar la Política de Seguridad.
5. Aprobar, tras cada proceso de apreciación del riesgo que se realice, el Plan de Tratamiento del Riesgo que se elabore.
6. Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del sistema.

7.4.2 Comité de Seguridad

El Comité de Seguridad de la Información de MUFACE coordina la seguridad de la información. Los miembros del Comité actúan con voz y voto y sus acuerdos se adoptan por mayoría simple de sus miembros, salvo que se establezca alguna otra mayoría cualificada.

Composición:

El Comité de Seguridad de la Información está compuesto por los siguientes miembros:

Presidente	Secretario General
Secretario	Responsable de Seguridad
Vocales	Responsable Unidad Informática
	Responsables Colectivo
	Responsable Prestaciones Sanitarias
	Responsable Prestaciones Sociales
	Responsable QSF
Asesores	Protección de datos
	Oficina de Seguridad
	Jefe Proyecto SGAD
	Personal Unidad Informática
	DPD

A requerimiento del Comité de Seguridad se convocará a cualesquiera otros responsables, propios o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el ENS y por la regulación en materia de Protección de Datos.

Funciones del Secretario:

- Convocar las reuniones del Comité de Seguridad de la información
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones del Comité de Seguridad de la Información:

1. Atender las inquietudes del Consejo de Dirección y de los diferentes departamentos en materia de seguridad de la información.

2. Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
3. Promover la mejora continua del sistema de gestión de la seguridad de la información.
4. Elaborar la estrategia de evolución de la Organización en lo que se refiere a seguridad de la información.
5. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
6. Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
7. Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
8. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
9. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
10. Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
11. Tomar decisiones estratégicas para la organización en materia de seguridad.
12. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
13. Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
14. Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por la dirección, según el artículo 11 del RD 311/2022 del 3 de mayo, que regula el Esquema Nacional de Seguridad en la Administración Electrónica.

15. Aprobar la normativa interna en el ámbito de la seguridad de la información que sea necesaria.
16. Elaborar y revisar el Plan de Adecuación al Esquema Nacional de Seguridad y las medidas necesarias para su aprobación por la dirección.
17. Implementar el Plan de Adecuación.
18. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables o entre diferentes áreas de MUFACE.
19. Recabar de los responsables de los distintos ámbitos de la seguridad informes regulares del estado de la seguridad de la organización y de las posibles incidencias que se produzcan.

7.4.3 Responsable de Seguridad

El Responsable de Seguridad de la Información gestiona el proceso de seguridad de la información.

Funciones:

1. Promover la conformidad con el Esquema Nacional de Seguridad en su ámbito de aplicación.
2. Proponer medidas encaminadas a mejorar la seguridad de la información: Elaborar, junto al Responsable del Sistema, planes de mejora de la seguridad y continuidad de sistemas, para su aprobación por el Comité de Seguridad de la Información
3. Firmar la Declaración de Aplicabilidad de acuerdo con lo previsto en el artículo 27 y en el anexo II del ENS.
4. Colaborar en la determinación de la categorización de los distintos sistemas en el marco del ENS: Recopilar los requisitos de seguridad de los Responsables de la Información y del Servicio y determinar la categoría del Sistema en el marco del ENS.
5. Asegurar que se llevan a cabo los análisis de riesgos periódicos, revisar sus resultados y supervisar el proceso posterior de gestión del riesgo y la elaboración de planes y medidas para gestionar los riesgos detectados.
6. Impulsar la realización de las auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, así como analizar

los informes de auditoría y elaborar las conclusiones a presentar a los responsables del servicio y a los responsables de la información para que adopten las medidas correctoras adecuadas.

7. Proponer al Comité de Seguridad, para su aprobación, la normativa de seguridad de la información de MUFACE.
8. Supervisar el cumplimiento de las políticas, normativas y procedimientos de seguridad establecidos y aprobar los Procedimientos Generales y Operativos de Seguridad de la Información, así como, las Instrucciones Técnicas.
9. Asegurar que la documentación de seguridad se mantenga organizada, actualizada y accesible.
10. Promover las actividades de concienciación y formación en materia de seguridad en el ámbito de MUFACE.
11. Elaborar informes periódicos de seguridad para el Comité que incluyan los incidentes más relevantes de cada período, así como cualquier otra documentación dentro de su ámbito de responsabilidad que el Comité necesite recabar para poder tomar decisiones en materia de seguridad de la información (por ejemplo, resumen de actuaciones en materia de seguridad, informes del estado de la seguridad del sistema y del nivel de riesgo residual al que está expuesto el sistema, etc).
12. Coordinar y controlar las medidas de seguridad tanto técnicas como organizativas que apliquen en virtud de lo dispuesto por el RGPD y la normativa relacionada, de cara a mantener la seguridad de la información y de los servicios prestados por los sistemas de información.

Para la ejecución de estas funciones podrá nombrar ***Responsables de Seguridad Delegados*** que, aun no siendo miembros del Comité de Seguridad de la Información de MUFACE, darán apoyo y asesoramiento al Responsable de Seguridad y ejecutarán aquellas tareas que éste les encomiende hasta el nivel técnico que sea necesario.

7.4.3.1 Responsables de Seguridad Delegados

Los Responsables de Seguridad Delegados ayudan al Responsable de Seguridad a gestionar el proceso de seguridad de la información.

Funciones:

1. Dar apoyo y asesoramiento al Responsable de Seguridad.
2. Ejecutar las tareas encomendadas por el Responsable de Seguridad y mantenerle informado de todos los aspectos de la seguridad TIC que debe conocer. El listado de las tareas que puede tener delegadas se encuentra detallado en el documento de definición del Comité de Seguridad de la información en el punto en el que se definen los Responsables de Seguridad Delegados (RSID).
3. Informar al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
4. Informar al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

7.4.4 Responsable del Servicio y de la Información

Funciones:

1. Determinar los niveles de seguridad de la información en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) en el ámbito de su Servicio o área, dentro del marco establecido en el Anexo I del ENS, previa propuesta del Responsable de la Seguridad.
2. Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Aprobar el riesgo residual resultante de aplicar los controles de seguridad.
3. Supervisar el uso adecuado y la protección de la información y responder de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
4. Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

5. Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
6. Aprobar el riesgo residual (el resultante una vez aplicado los controles de seguridad).

7.4.5 Responsable del Sistema

El Responsable del Sistema es la persona que toma las decisiones operativas: arquitectura del sistema, requisitos a tener en cuenta, instalaciones y operación del día a día.

Dado que la operación de los sistemas de MUFACE está delegada en la Secretaria General de Administración Digital (SGAD), se crea la figura de ***Responsable del Sistema Delegado***, siendo éste quien debe operar y mantener el sistema.

Funciones:

1. Planificar e implantar las medidas necesarias para garantizar la seguridad del servicio durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad y Responsable de Seguridad Delegado.
2. Definir tipología y política de gestión del sistema y aprobar cualquier modificación sustancial de la configuración de cualquier elemento del sistema.
3. Asesorar al Responsable de la Seguridad, a los Responsables de la Información y a los Responsables del Servicio en la realización de los análisis de riesgos del sistema.
4. Establecer planes de continuidad, contingencia o emergencia y simulacros.
5. Acordar la suspensión del uso de determinada información o prestación de servicio si hay vulnerabilidades graves en el sistema, decisión previamente acordada con el Responsable de Seguridad.
6. Conexión y desconexión de equipos/usuarios.
7. Aprobar cambios operativos.
8. Configuración hardware y software.

7.4.6 Delegado de Protección de Datos (DPD)

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos (DPD) tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben con relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el RGPD y en otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD;
- Cooperar con la autoridad de control;
- Atender las consultas que los interesados realicen a la entidad, ya sea para cuestiones relativas al tratamiento de sus datos o para el ejercicio de sus derechos;
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

No recae en el ámbito del comité de seguridad la asignación del responsable de protección de datos, pero sí debe supervisar la existencia del citado responsable y el cumplimiento de la normativa.

8 Datos de Carácter Personal

MUFACE trata datos de carácter personal de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre

circulación de estos datos y la Ley Orgánica 3/2018 cuyo objeto es adaptar al mismo el ordenamiento jurídico español y completar sus disposiciones.

La Organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De este modo, con la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos. De este análisis de riesgos se pueden derivar medidas que se superpongan a las ya descritas como obligatorias para el ENS según la categorización del sistema.

9 Análisis y Gestión de Riesgos.

Todos los sistemas sujetos a la presente Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Responsable de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para MUFACE, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD. El responsable o el encargado del tratamiento,

asesorado por el Delegado de Protección de Datos, realizará un análisis de riesgos conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una Evaluación de Impacto en la Protección de Datos (EIPD). Del resultado de ese análisis pueden derivarse medidas adicionales a implantar.

MUFACE utiliza la metodología Magerit para analizar los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda documentado en un documento de Análisis de Riesgos.

La Organización determina los niveles de riesgo a partir de los cuales toma acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implementar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de MUFACE es la responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

En el caso de las medidas implantadas en el ENS, si el análisis de riesgos establece medidas más importantes, se añadirán éstas a las descritas en el ENS.

10 Desarrollo de la Política de Seguridad de la Información

10.1 Instrumentos de Desarrollo y Gestión de la Documentación

Esta Política de Seguridad de la Información se desarrollará a través de los siguientes instrumentos:

- **Normas de Seguridad TIC (SGSI):** Desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

- **Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información (PGS):** Establecen la manera en que la Organización establece, implementa, mantiene y mejora de manera continua el SGSI.
- **Procedimientos Operativos de Seguridad (POS):** Documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada actividad o cumplir con un requisito conforme a los principios de seguridad de la organización y los procesos internos en ella establecidos.
- **Instrucción Técnica de Seguridad (ITS):** Se redactan cuando en relación con una actividad es necesario un mayor nivel de concreción que el establecido en un POS. Es un documento de carácter técnico en el que se describe, con el nivel de detalle preciso (quién, cómo, cuándo y dónde), el desarrollo de una determinada actividad y que se emiten para poder cumplir las políticas establecidas en los POS.

10.2 Estructura General

El desarrollo de la normativa de seguridad en su conjunto se llevará a cabo basándose en el análisis de riesgos y aspectos específicos de la Seguridad de la Información tales como las medidas de seguridad indicadas en el Anexo II del ENS:

- **Marco organizativo:** orientado a administrar la seguridad de la información dentro de MUFACE. Partiendo de la presente Política de Seguridad de la Información se desarrollará el resto del marco normativo de seguridad.
- **Marco operacional**: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
- **Medidas de protección**: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

10.3 Gestión de la documentación

La gestión de la documentación relacionada con la seguridad de la información tendrá en cuenta el ciclo de vida de esta (generación, aprobación, modificación), de modo que se establezcan distintas responsabilidades en cada fase del ciclo de vida.

En este sentido, la gestión de la documentación contará con los siguientes roles relacionados:

- Consejo de Dirección (Dirección)
- Comité de Seguridad de la Información (CSIM)
- Responsable de Seguridad de la Información (RSI)
- Responsable de Seguridad Delegado (RSID)
- Responsable del Sistema (RS)
- Responsable del Sistema Delegado (RSD)

De acuerdo con lo anterior, en función del tipo de documento y el ciclo de vida, se ha establecido la siguiente matriz:

	Generación	**Aprobación**	**Modificación**
Política de Seguridad de la Información	CSIM	Dirección	CSIM
Plan de Adecuación al Esquema Nacional de Seguridad	CSIM	Dirección	CSIM
Informes periódicos de seguridad para CSIM	RSI	CSIM	RSI
Normativas de seguridad de la información	RSID - RS	RSI-CSIM	RSID - RS
Procedimientos Generales SGSI	RSID – RS/RSD	RSI	RSID – RS/RSD
Procedimientos Operativos de Seguridad e Instrucciones Técnicas	RS/RSD	RSID/RSI	RS/RSD
Documentación de seguridad del sistema	RS/RSD	RSID/RSI	RS/RSD
Planes de continuidad, contingencia o emergencia	RS/RSD	RSID/RSI	RS/RSD

	Generación	Aprobación	Modificación
Planes de mejora de la seguridad	RSID – RS/RSD	RSI-CSIM	RSID – RS/RSD

10.4 Sanciones previstas por incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los preceptos incumplidos.

El procedimiento y las sanciones para aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

11 Seguridad de la Información

Se dispondrá un sistema de etiquetado o nombrado para los documentos, de manera que el destinatario de la información pueda conocer el tipo de información que contiene el documento, departamento o área a la que pertenece, categoría de información que contiene, existencia de datos personales o cualquier otra información que resulte relevante en materia de datos personales.

11.1 Calificación de la Información

Toda la información que obra en los sistemas de información responsabilidad de MUFACE deberá contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, que garanticen la protección respecto a todas las dimensiones de la seguridad. Estas medidas de seguridad se establecerán de acuerdo con unos criterios basados en el uso de la información y su difusión.

A continuación, se establece una propuesta de niveles de calificación de la información (etiquetado) en base a su grado de confidencialidad (teniendo en cuenta su uso y su difusión, como ya se ha dicho) y que sirve tanto si está en formato electrónico como en papel.

Calificación (etiqueta)	Tipo de información y disponibilidad de ésta
Sin calificar	Información que no ha podido ser calificada, estando su contenido accesible a cualquier persona
Uso público	Información elaborada expresamente para su difusión pública
Uso interno	Información que debe estar disponible únicamente para las personas que se autentiquen con una cuenta @[empresas.]MUFACE.es
Difusión restringida	Información que quedará disponible únicamente para las personas o dominios que el usuario que etiquete la información decida; dichas personas deberán superar un proceso de autenticación para poder acceder a la información
Difusión prohibida	Información disponible únicamente en las instalaciones de MUFACE y para un conjunto extremadamente reducido de personas, autorizadas al acceso conforme a un procedimiento estricto

Esta propuesta podrá ser desarrollada con mayor detalle y ejemplos en una Norma específica de calificación y protección de la información.

Toda la documentación, digital o impresa, debe indicar la calificación de la información que contiene, salvo la información catalogada como pública.

Para dicha calificación se definirá un Procedimiento de Calificación de la Documentación.

La calificación de la información debe tener en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella.

12 Obligaciones del Personal

Todos los miembros de MUFACE tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información.

Así mismo, deberán conocer la Normativa de Seguridad que la desarrolla en la medida que les sea de aplicación en el desempeño de sus cometidos.

El Comité de Seguridad de la Información dispondrá los medios necesarios para que tanto la Política como la Normativa lleguen a los destinatarios concernidos.

Para ello, además de que la política esté disponible en los sistemas de información de MUFACE, al menos una vez al año, se recordará a todo el personal la necesidad de su conocimiento y cumplimiento y se notificará cualquier cambio que se haya producido.

Así mismo, se establecerá un programa de concienciación continua para todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será recomendada antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

13 Terceras Partes

Cuando MUFACE utilice servicios o ceda información de/a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que afecte a dichos servicios o información. La tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. De igual modo deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el ENS cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el ENS, cuando se trate de sistemas de categorías MEDIA o ALTA, en los servicios concernidos.

Cuando MUFACE preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable del Sistema que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Comité de Seguridad antes de seguir adelante.

13.1 Terceras Partes como Servicios Externalizados de Seguridad

En el caso de servicios externalizados de seguridad, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con el mismo.

14 Desarrollo del SGSI, Revisión y Auditorias

La Dirección aprobará el desarrollo de un sistema de gestión de la seguridad de la información (SGSI) que será establecido, implementado, mantenido y mejorado conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del ENS. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas del ENS, prestando especial atención a las guías publicadas por el Centro Criptológico Nacional como desarrollo de las medidas y controles de seguridad.

Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en la Declaración de Aplicabilidad, y serán proporcionales a la criticidad de la información a proteger y a su clasificación.

El Comité de Seguridad de la Información revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección. Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará cada dos años, según un plan de auditorías desarrollado por el Comité de Seguridad.

Anexo 1. Acrónimos

ACRÓNIMOS	
CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
CSIM	Comité de Seguridad de la Información de MUFACE
PSI	Política de Seguridad de la Información
RSI	Responsable de Seguridad de la Información
RSID	Responsable de Seguridad de la Información Delegado
RS	Responsable del Sistema
RSD	Responsable del Sistema Delegado
STIC	Sistemas de Tecnologías de la Información y las Comunicaciones
CERT	Equipo de respuesta ante incidentes *(Computer Emergency Response Team)*
DPD	Delegado de Protección de Datos
RGPD	Reglamento General de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
EIPD	Evaluación de Impacto en la Protección de Datos
POS	Procedimientos Operativos de Seguridad
ITS	Instrucción Técnica de Seguridad