NORMA DE USO DEL CORREO ELECTRÓNICO CORPORATIVO

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

INTRODUCCIÓN **4**

2 ÁMBITO DE APLICACIÓN **4**

3 CONTEXTO DE LA PRESENTE NORMA **4**

4 TERMINOLOGÍA RELEVANTE **5**

5 PROVISIÓN DEL SERVICIO **6**

6 NORMAS DE USO **7**

6.1 Usos autorizados 7

6.2 Usos no autorizados 7

7 BUENAS PRÁCTICAS **8**

8 MEDIDAS DE CONTROL **9**

9 INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD **10**

10 REVISIÓN DE LA NORMA **10**

11 RESPONSABILIDAD POR INCUMPLIMIENTO **10**

12 ANEXO I: REFERENCIAS NORMATIVAS **11**

12.1 Medida org.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

1 Introducción

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de aplicación al sector público, según el artículo 2 de la Ley 40/2015 del 1 de octubre, y según el artículo 156.2, establece los principios básicos y requisitos mínimos requeridos para proteger la información. Las Administraciones Públicas deberán aplicarlo para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

MUFACE dispone como herramienta de trabajo del servicio de correo electrónico, entendiendo como tal el servicio de red que permite a los usuarios enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos.

Para garantizar el uso racional y seguro de este recurso, debe conocerse la norma donde se especifica qué se considera un uso correcto del servicio. Con ese objeto, se redacta el presente documento, que describe la Norma de uso del correo electrónico corporativo.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (interno y externos) que tengan acceso a los sistemas de correo de MUFACE.

3 Contexto de la presente norma

La presente norma de uso del servicio de correo electrónico corporativo pertenece a una serie de documentos que describen la normativa de uso seguro de los recursos informáticos de MUFACE, relacionada con la seguridad en los puestos de trabajo, la red corporativa, los equipos portátiles, las aplicaciones informáticas, así como sobre el acceso y tratamiento de la información por parte de los usuarios.

La citada serie de documentos se integran a su vez dentro del desarrollo normativo de seguridad derivado de la Política de Seguridad de la Información (PSI) de MUFACE, que está

alineado con los principios básicos y los requisitos mínimos exigidos por el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS).

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

4 Terminología relevante

A lo largo del texto de los documentos de desarrollo normativo de seguridad requeridos por la PSI de MUFACE se citan una serie de definiciones, entre ellas algunas figuras o roles, a los que se aludirá con letra cursiva siguiendo la siguiente nomenclatura:

- **Usuario:** la persona o sistema que utiliza los sistemas de información de MUFACE, y/o a la información contenida en ellos.

- **Unidad TIC**: unidad encargada del desarrollo, mantenimiento y explotación del sistema de información al que estemos haciendo referencia.

- **Responsable del Sistema**: según define la PSI, esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes. Por tanto, según esta definición, recae sobre el titular de la Unidad TIC.

- **Responsable de Seguridad**: según define la PSI, la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios.

- **Norma específica de cada ámbito:** Una norma específica desarrolla con mayor detalle la norma correspondiente de aplicación general dentro del ámbito de competencia de cada Responsable de Seguridad, si se considera necesario por parte de éste. En caso de existencia de norma específica y de discrepancia entre ésta y la norma general, prevalecerá lo indicado en la específica para la información y servicios afectados por los sistemas de información gestionados por el ámbito de competencia del Responsable de Seguridad correspondiente.

5 Provisión del servicio

El sistema de correo electrónico, incluyendo todos los mensajes generados o manejados por él y las copias de respaldo, es propiedad de MUFACE, ofreciendo un servicio que pone a disposición del personal para un mejor cumplimiento de sus obligaciones laborales.

MUFACE proporcionará a cada usuario una cuenta de correo electrónico, accesible mediante un usuario y clave personal, que deberá conocer y custodiar. Será responsabilidad de cada usuario las actividades realizadas con sus cuentas de acceso.

Se podrá establecer un sistema de cuotas que limite la capacidad de almacenamiento de mensajes en el servidor por parte de cada usuario.

Se podrá limitar el tamaño de los ficheros que se adjunten a los mensajes, pudiendo estos no cursarse y ser rechazados en el caso de que se supere el mismo.

La Unidad TIC correspondiente se reserva el derecho a fijar los aplicativos clientes autorizados para el uso de este servicio.

Se realizarán copias de seguridad periódicas de la configuración del sistema y de sus datos, pero no se garantiza la permanencia en los sistemas del contenido de los buzones con una antigüedad mayor de la definida por la norma específica de cada ámbito. En el caso de no existir esa definición en la norma específica, la antigüedad será de 2 meses. Por ello cada usuario deberá responsabilizarse de efectuar copias de los mensajes o datos asociados cuya conservación considere necesaria.

Debe de tenerse en cuenta que, por la propia concepción de los protocolos y estándares utilizados en Internet, el correo electrónico no es un medio de comunicación seguro, puesto que no garantiza la autenticidad del emisor, ni la confidencialidad e integridad de los mensajes, que no viajan cifrados y son susceptibles de ser interceptados por terceros. Por ello, deberán utilizarse mecanismos de firma y de cifrado adicionales o cualquier otro mecanismo autorizado para la transmisión de correos con información sensible. La unidad TIC correspondiente podrá asesorar sobre posibles mecanismos para ello.

Con la finalización de la relación de servicio con MUFACE por parte de un usuario se interrumpirá su acceso a la cuenta asignada.

6 Normas de Uso

6.1 Usos autorizados

En general, el uso del sistema de correo está restringido a las funciones que correspondan al puesto de trabajo que desempeña el usuario.

Se permite la suscripción a listas de distribución y a otras formas de los servicios de la suscripción del correo electrónico relacionadas con las funciones del puesto de trabajo.

6.2 Usos no autorizados

Está prohibido utilizar el sistema de correo en los siguientes casos:

1. Crear o intercambiar mensajes ofensivos u obscenos de cualquier clase, incluyendo material pornográfico.
2. Enviar correos electrónicos que promuevan la discriminación en base a la raza, el sexo, nacionalidad, la edad, el estado civil, la orientación sexual, la religión, la discapacidad, o cualquier otro motivo.
3. Enviar correo electrónico que contenga amenazas o mensajes violentos o intimidatorios.
4. Enviar mensajes con información confidencial a destinatarios no autorizados, con especial atención a los envíos al exterior de la SEAP (como, por ejemplo, a proveedores), para los que además se deberá proteger la información sensible mediante cifrado.
5. Facilitar el acceso a la cuenta y contraseña personal a terceras personas. En particular, nunca se deberá contestar a ningún correo recibido que solicite información de acceso a los sistemas de MUFACE (nombre de usuario, claves, etc.), ni atender a las instrucciones que incluya (pinchar en algún enlace, abrir un fichero adjunto, etc.).
6. Enviar mensajes de correos no solicitados (Spam, Phishing, cadenas de cartas, publicidad, etc.).
7. Enviar mensajes con fines políticos, comerciales, de entretenimiento o para obtener lucro económico.

8. Enviar sin autorización correos de forma masiva, y en particular realizar un uso abusivo de las listas de correo.
9. Almacenar o enviar mensajes que contengan material protegido bajo las leyes de propiedad intelectual, sin el consentimiento de su(s) autor(es).
10. Enviar virus o software malicioso, o, en general, realizar cualquier uso abusivo o malintencionado del sistema que ponga en riesgo la seguridad de los sistemas de información.
11. Abrir un archivo anexo de un mensaje de correo sin que se analice antes con el software antivirus corporativo. En particular no deberán abrirse aquellos provenientes de fuentes no confiables.
12. Interceptar o hacer públicos los mensajes de otro usuario, o alterar su contenido, sin su consentimiento expreso y por escrito.
13. Utilizar la cuenta de correo electrónico asignada a otro usuario sin su consentimiento expreso y por escrito.
14. Inscribir la cuenta de correo en listas no relacionadas con las funciones de MUFACE.
15. Utilizar el servicio para la comisión de cualquier otro acto tipificado como delito, o en general, cualquier actividad ilícita.

7 Buenas prácticas

En el caso de que se necesite difundir información de manera masiva, se recomienda ponerse en contacto con los responsables del servicio (mediante los métodos habilitados para la notificación de incidencias) quienes orientarán sobre la manera más adecuada de hacerlo.

Se recomienda que los documentos que se anexen en los correos sean lo más reducidos posibles, sobre todo cuando estos van dirigidos a numerosos destinatarios.

A este respecto, se indica que al realizar el escaneado de documentos para su envío por correo, deberían configurarse en lo posible en blanco y negro y en la menor precisión que

permita su correcta visualización. Asimismo, es deseable que se compriman previamente a su envío.

Se debe revisar periódicamente el tamaño de ocupación del buzón de correo electrónico con el fin de evitar llegar a la cuota máxima. Para ello se recomienda mover los mensajes de correo a carpetas locales o al tipo de almacenamiento aconsejado por la Unidad TIC. Hay que tener en cuenta que todas las carpetas del buzón de correo utilizan espacio asignado al mismo, por lo que hay que revisar, entre otras, la carpeta de elementos enviados y vaciar la papelera de manera periódica.

Debe extremarse la precaución en el caso de acceso al sistema de webmail (acceso vía web a la cuenta de correo electrónico) desde ordenadores externos a MUFACE. No deben activarse las opciones de autocompletar ni de recordar contraseñas. Una vez finalizada la sesión se debe borrar la información temporal almacenada, como cookies, formularios, contraseñas, historial y archivos temporales de Internet, para evitar accesos indeseados por terceras personas.

En lo referente a la utilización del correo electrónico corporativo desde dispositivos móviles se estará a lo dispuesto en la Norma que regula el uso de estos dispositivos.

8 Medidas de control

La SEAP se reserva el derecho de aplicar las medidas técnicas y organizativas necesarias para garantizar el buen uso del servicio. En caso de detectarse el incumplimiento de la presente norma, o de incidentes de seguridad derivados del uso del sistema de correo que afecten a los sistemas de información, se podrá acordar la supresión o limitación del servicio de correo a los usuarios involucrados.

El correo intercambiado a través del servicio de correo se inspeccionará y filtrará de manera automática a través de los sistemas de antivirus y antispam corporativos. Estos sistemas podrán, de manera automatizada y sin menoscabo de la privacidad, rechazar, bloquear o eliminar parte o la totalidad del contenido de los mensajes en los que se haya detectado alguna amenaza.

No obstante, en ningún caso se inspeccionará de manera manual el contenido de los mensajes intercambiados salvo que:

- Sea solicitado a MUFACE por las autoridades competentes bajo la investigación de una posible comisión de delitos.
- Un usuario solicite una revisión de correos dirigidos a él que hayan sido retenidos por los sistemas antivirus y antispam debido a un posible falso positivo en el análisis.

9 Información sobre incidentes de seguridad

Los usuarios deberán informar de cualquier incidente o anomalía relacionados con el servicio de correo electrónico o con su seguridad a través de los medios habilitados por MUFACE para la notificación de incidencias especificados en las intranets correspondientes.

Como ejemplos de posibles incidentes: recepción de correos sospechosos o no deseados, sospecha de la suplantación de la identidad en el envío de mensajes, solicitud de desbloqueo de mensajes considerados lícitos, etc.

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 Responsabilidad por incumplimiento

Todos los usuarios del servicio de correo electrónico de MUFACE están obligados al cumplimiento de las pautas de conducta establecidas en la presente norma, pudiéndose derivar de su incumplimiento la pertinente responsabilidad en el ámbito disciplinario, si a ello hubiera lugar en aplicación de las disposiciones reguladoras del estatuto jurídico del usuario. La detección de actuaciones irregulares, ilícitas o ilegales podrá acarrear la

iniciación de las medidas disciplinarias oportunas y, en su caso, de las acciones legales correspondientes.

12 Anexo I: Referencias normativas

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.

12.1 Medida org.2

Se dispondrá de una serie de documentos que describan:

- El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

12.2 Medida mp.s.1

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
- Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

- Correo no solicitado, en su expresión inglesa «*spam*».

- Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
- Código móvil de tipo micro-aplicación, en su expresión inglesa «*applet*».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]).

Estas normas de uso contendrán:

- Limitaciones al uso como soporte de comunicaciones privadas.
- Actividades de concienciación y formación relativas al uso del correo electrónico.