NP.02 NORMAS DE USO DEL CORREO ELECTRÓNICO CORPORATIVO

Documento de uso interno

ÌNDICE

1 Objetivo 4
2 Ámbito de aplicación 4
3 Vigencia 4
4 Revisión y evaluación 5
5 Normas previas 5
6 Normativa 5
6.1 Definiciones 5
6.2 Dominio de correo 6
6.3 Tipos de cuentas de correo 6
6.4 Nomenclator 7
6.5 Usuarios del servicio de correo 9
6.6 Gestión de las cuentas de correo 9
6.6.1 Alta en el servicio de correo 9
6.6.2 Gestión de cuentas de correo 9
6.6.3 Baja en el servicio de correo 10
6.6.4 Caducidad de las cuentas de correo 10
6.7 Encaminamiento del correo 11
6.8 Gestión y mantenimiento del servicio de correo 11
6.9 Copias de seguridad 11
6.10 Derechos de los usuarios 12
6.11 Obligaciones de los usuarios 12
6.12 Documentación y notificación de incidencias 13
6.13 Uso adecuado y seguro del correo 13
7 Prevención contra SPAM 16
8 Modelo de aceptación y compromiso de cumplimiento 17
9 Referencias 17
Apéndice: Lenguaje de género 18

CONTROL DE VERSIONES

<table>
<tr><td>Revisión</td><td colspan="2">Fecha</td><td>Motivo del Cambio</td></tr>
<tr><td>1.0</td><td colspan="2">1/11/2023</td><td>Versión inicial</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Realizado y revisado:
SICUE / Responsable de seguridad</td><td colspan="2">Aprobado: Comité de Seguridad
Fecha: 17/11/2023</td></tr>
</table>

1 Objetivo

El objetivo de la presente norma es regular el **acceso y utilización del correo electrónico (e-mail)** por parte de los usuarios de los Sistemas de Información de la Universidad de Extremadura, desde las distintas sedes de la Universidad de Extremadura o a través de ellas, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

> La presente Normativa General de Utilización de los Recursos y Sistemas de Información de la Universidad de Extremadura deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

Este documento se considera de uso interno de la Universidad de Extremadura (a partir de ahora, UEx) y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad/Comité de Seguridad.

2 Ámbito de aplicación

Esta Norma se aplica a todo el ámbito de actuación de la UEx, y sus contenidos traen causa de las directrices de carácter más general definidas en el documento **PO.01 Política de Seguridad de la Información de la Universidad de Extremadura** (D.O.E. 8 de junio de 2023)

La presente Norma **será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la UEx**, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la UEx.

3 Vigencia

La presente Norma ha sido aprobada por el Comité de Seguridad de la UEx, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la UEx pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la UEx.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4 Revisión y evaluación

La gestión de esta Normativa corresponde al Comité de Seguridad que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente normativa, que se someterá, de haber modificaciones, a aprobación.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5 Normas previas

Las presentes **Normas de Uso del Correo Electrónico (e-mail) en la UEx** complementa, en sus aspectos específicos, a la **Normativa General De Utilización De Los Recursos Y Sistemas De Información De La UEx**, por lo que tal normativa general se aplicará en los aspectos no señalados en aquella.

6 Normativa

6.1 Definiciones

En el contexto de esta norma, se entiende por:

a. *Correo electrónico corporativo de la UEx*: Servicio prestado bajo dominio titularidad de la UEx y proporcionado por la universidad al conjunto de usuarios integrantes de su comunidad universitaria y, en particular, a los empleados públicos a su servicio.

b. *Buzón de correo electrónico*: Depósito que sirve para almacenar correos electrónicos.

c. *Cuenta de correo personal*: Cuenta de correo electrónico bajo el dominio de la UEx asignada a una persona que incluye un buzón de correo de uso exclusivo.

d. *Cuenta de correo electrónico activa*: Cuenta de correo electrónico corporativo que tiene acceso a su buzón y permite tanto enviar como recibir mensajes de correo.

e. *Cuenta de correo electrónico desactivada*: Cuenta de correo electrónico corporativo extinguida al término de su vigencia y con arreglo a lo previsto en esta norma. Cuando una cuenta está desactivada, no permite acceder a su buzón, ni enviar ni recibir mensajes de correo.

f. *Cuenta de correo electrónico abandonada*: Cuenta de correo en la que la persona usuaria no atiende los avisos de renovación una vez llegado a su caducidad.

g. *Encaminamiento de correo electrónico*: Procesos y configuraciones necesarias para decidir e indicar la ruta a seguir por los correos enviados o recibidos en un servicio de correo.

h. *DIR3*: Es el Directorio de Unidades Orgánicas y Oficinas de Registro de las Administraciones Públicas (AAPP).

6.2 Dominio de correo

El servicio de correo electrónico corporativo prestado por la UEx permite el uso de buzones de correo bajo los siguientes dominios de titularidad de la UEx:

- *<unex.es>*
- *<alumnos.unex.es>*

Por tanto, las cuentas de correo tomarán la forma *<usuario@unex.es>* o *<usuario@alumnos.unex.es>*. La asignación de nombres de usuario la realizará el SICUE de acuerdo a un procedimiento que se especifica en la sección 6.4, incorporando información identificativa del usuario (nombre, apellidos, etc) y garantizando la unicidad de identificadores.

6.3 Tipos de cuentas de correo

Las cuentas de correo electrónico son para uso estrictamente profesional y estarán asociadas a una persona responsable de la misma. Las cuentas de correo electrónico pueden ser de dos tipos:

1) Cuentas personales: Cuentas asociadas a una persona usuaria de correo. Se distinguen dos subtipos:

    a) Cuenta de correo personal principal. Cuenta de correo personal que podrá disfrutar todas aquellas personas que pertenecen a la comunidad universitaria. Sólo se permite una cuenta de correo personal principal.

    b) Cuenta de correo personal secundaria. Para cualquier persona que tenga una cuenta de correo personal principal, se contempla posibilidad de creación de hasta 5 cuentas de correo adicionales. Estas cuentas pueden utilizarse para diferentes fines (eventos temporales, etc.).

Este tipo de cuentas tendrán una vigencia de 1 año, y pasarán a ser desactivadas una vez cumplido el plazo, salvo renovación expresa por parte del usuario.

2) Cuentas de correo institucional. Se trata de cuentas de correo asociadas a puestos y cargos de las distintas unidades organizativas de la UEx. Este tipo de cuentas se solicitarán cuando sean necesarias y estén justificadas, y estarán vinculadas a una unidad organizativa existente en DIR3, siendo la persona responsable de dicha unidad la encargada de la cuenta.

3) Cuentas Organizativas. Están orientadas fundamentalmente a unidades, grupos y servicios. Pueden ser utilizadas por una o varias personas conjuntamente y son gestionadas por un responsable. Por consiguiente, este tipo de cuentas no están asociadas a cargos o personas.

6.4 Nomenclator

La asignación de nombres de usuario para las cuentas de correo electrónico se realizará de una forma ordenada, siguiendo criterios específicos según el tipo de cuenta.

Cuentas institucionales

Cuenta	Identificador
Rector	*rector*
Gerente	*gerente*
Secretario General	*secgral*
Vicerrectores	*vr* + identificador del vicerrectorado
Adjuntos en los vicerrectorados	*ad* + identificador del vicerrectorado
Servicios, Secretariados, Oficinas, Unidades	nombre identificativo del servicio, secretariado, etc. Sugerido por el solicitante y aprobado por el SICUE.
Centros de la universidad:	
Decano y Director	*dircent* + 4 letras identificativas del centro.
Vicedecanos y Subdirectores	*subdircent* + las 4 letras identificativas del centro + '_' + nombre identificativo de la subdirección o vicedecanato.
Secretario Académico	*seccent* + las 4 letras identificativas del centro
Administrador	*administrador_* + las 4 letras identificativas del centro

Biblioteca	*biblioteca_* + las 4 letras identificativas del centro
Conserjería	*conserjeria_* + las 4 letras identificativas del centro
Técnico de informática	*tecnicoinformatica_* + las 4 letras identificativas del centro
Consejo de estudiantes del centro	*conalum* + las 4 letras identificativas del centro
Departamentos:	
Director	*dirdpto* + 4 letras identificativas del departamento.
Secretario	*secdpto* + 4 letras identificativas del departamento.
Consejo de Estudiantes:	
Dirección del consejo	*consejoestudiantes*
Secretaria	*secretariaceuex*
Tesorería	*tesoreroceuex*

Todos los nombres serán asignados y/o aprobados por el SICUE.

Cuentas personales

El nombre del usuario que identifica a las cuentas de correo personales principales será asignado por el SICUE, para utilizar nombres identificativos ligados al nombre del usuario al que pertenecen. Se seguirán las reglas siguientes:

- Se sustituyen los caracteres acentuados por los mismos caracteres sin acentuar.
- Se elimina cualquier carácter que no sea una letra del abecedario.
- Se sustituye la letra “ñ” por la letra “n”.
- Se aplican los siguientes patrones, seleccionando aquel que no supere los 20 caracteres de longitud y no esté en uso:
    - "primer_nombre""segundo_nombre"."primer_apellido"
    - "primer_nombre"."primer_apellido"
    - "primer_nombre""inicial_segundo_nombre"."primer_apellido"
    - "segundo_nombre"."primer_apellido"
    - "inicial_primer_nombre""segundo_nombre"."primer_apellido"
- Sólo en caso de imposibilidad de aplicación de cualquiera de las estrategias anteriores se procederá a una asignación manual del nombre la cuenta, manteniendo la filosofía de que

exista una relación estrecha entre el nombre del usuario y su nombre de cuenta

Las cuentas personales secundarias pueden ser elegidas por los propios usuarios, pero serán examinadas y aprobadas por el SICUE (para comprobar que son adecuadas, coherentes y no entran en conflicto con otras cuentas).

6.5 Usuarios del servicio de correo

Se consideran usuarios del servicio de correo a los siguientes colectivos:

a) Personal Docente e Investigador, Personal de Administración y Servicios, y Estudiantes de la UEx.

b) Egresados y egresadas de la UEx, durante el periodo de tiempo determinado por la duración de las cuentas de correo.

c) Todas aquellas personas que mantienen una vinculación temporal con la UEx, cuya actividad requiera de disponer de una cuenta de correo electrónico. En estos casos, se requerirá la autorización explícita del Vicerrectorado con competencias TIC.

6.6 Gestión de las cuentas de correo

6.6.1 Alta en el servicio de correo

El alta en el servicio de correo electrónico corporativo se produce con la creación de la primera cuenta de correo personal principal y activa en alguno de los dominios de la UEx. El alta se realizará siguiendo uno de los siguientes procedimientos:

a) En el caso de estudiantes, con ocasión de la primera matrícula.

b) En el supuesto de empleados públicos de la UEx, al establecerse la correspondiente relación de servicios y mediante las aplicaciones corporativas existentes.

c) En el supuesto de otros colectivos distintos de los señalados en los apartados anteriores, por medio de las aplicaciones corporativas habilitadas al efecto y autorizadas por el vicerrectorado competente en TICs.

En tanto se disponga de la condición de estudiante o de empleado público al servicio de la UEx, no se podrá renunciar a la cuenta de correo personal principal asignada, ni obtener su cancelación o desactivación.

La creación y gestión del resto de cuentas se realizará a través del procedimiento de Gestión de Cuentas de correo descrito a continuación.

6.6.2 Gestión de cuentas de correo

Gestión de credenciales.

La UEx pone a disposición de los usuarios una aplicación general para la Gestión de las Credenciales; dicha aplicación se accede en la dirección: https://www.unex.es/organizacion/servicios-universitarios/servicios/siue/funciones/servicio_usuario/gestion-de-credenciales.

Mediante esta aplicación, los usuarios pueden realizar todas las funciones requeridas para gestionar sus credenciales: altas de direcciones de correo electrónico, cambios de contraseña, desbloqueo de cuentas, etc. Actualmente, el acceso a esta aplicación se realiza mediante certificado electrónico reconocido o alternativamente mediante un sistema de autenticación de un solo uso.

Los cambios de titularidad de las cuentas institucionales serán realizados exclusivamente por personal autorizado del SICUE, previa petición del interesado a través del servicio CAU (https://cau.unex.es).

6.6.3 Baja en el servicio de correo

La baja en el servicio de correo electrónico corporativo de un usuario se producirá cuando deje de tener cuentas de correo electrónico personal activas.

6.6.4 Caducidad de las cuentas de correo

Todas las cuentas de correo electrónico corporativo tienen una fecha de caducidad determinada en función del colectivo al que pertenezca la persona usuaria y del tipo de relación que mantenga con la UEx.

En todo caso, cuando se extinga la relación con la UEx en cuya virtud se dispone de cuenta de correo personal, la cuenta correspondiente pasará a disponer de un plazo de vigencia general de 30 días a contar desde el día siguiente al de la extinción de la relación jurídica habilitante, a excepción de que la causa de la extinción de la relación sea por jubilación. En estos casos, el plazo de vigencia será de 365 días y el usuario, de forma personal, podrá renovar su cuenta a través de las opciones que se describen a continuación. Las cuentas secundarias serán eliminadas en el plazo máximo de 15 días tras la finalización de la relación que mantenga con la UEx. Las cuentas organizativas serán traspasadas en el mismo plazo que las anteriores. Las cuentas secundarias serán eliminadas en el plazo máximo de 15 días tras la finalización de la relación que mantenga con la UEx. Las cuentas organizativas serán traspasadas en el mismo plazo que las anteriores.

a) La UEx enviará sucesivos avisos a los usuarios con antelación de treinta, siete y un día respecto de la fecha prevista para la caducidad de la cuenta. Si no se ha obtenido respuesta por parte del usuario, luego de 14 días desde la fecha de caducidad se procederá a la desactivación de la cuenta.

b) No serán estimadas las pretensiones de reactivación de cuentas desactivadas, excepto en los siguientes supuestos:

1. Cuando la persona interesada acredite la concurrencia de causa justificada que le hubiera impedido la renovación en el tiempo previsto al efecto, en supuestos tales, con carácter enunciativo, como los debidos a enfermedad de larga duración, accidente u otros de fuerza mayor que sean fundadamente apreciados por el vicerrectorado competente en TICs.
2. Cuando la persona titular de la cuenta vuelva a tener relación con la UEx, que le otorgue el derecho a contar con una cuenta de correo.

Los buzones con los mensajes de las cuentas de correo electrónico corporativo desactivadas y que no haya sido objeto de solicitud de reactivación por sus propietarios serán eliminados del servicio pasado un año desde su desactivación. Así mismo, será anulada la suscripción de la dirección de correo de las listas de correo de la UEx a las que pudiera estar suscrita. .

6.7 Encaminamiento del correo

El encaminamiento de mensajes hacia y desde la UEx se efectuará a través de un sistema, la estafeta central, que será gestionado directamente por el SICUE de la UEx.

El resto de las estafetas de la UEx no podrán recibir o enviar correo directamente desde o hacia Internet, sino que solo podrán hacerlo a través de la estafeta central y deberán desaparecer en el plazo máximo de un año desde la entrada en vigor de esta normativa.

6.8 Gestión y mantenimiento del servicio de correo

La UEx, a través de sus servicios técnicos, efectuará las tareas de mantenimiento precisas para el correcto funcionamiento del servicio de correo, así como para la optimización de su operativa y de su rendimiento.

Las tareas de mantenimiento que comporten interrupción u otras incidencias sobre la operativa del servicio serán comunicadas con antelación suficiente a los usuarios afectados, por medio de mensajes de correo electrónico u otros medios adecuados, y se procurará que su realización se verifique en los días y horas que menores inconvenientes pueden ocasionar.

6.9 Copias de seguridad

Se realizará copia de seguridad de los siguientes elementos integrantes del servicio de correo electrónico corporativo:

a) Programas y archivos de configuración del propio servicio.

b) Archivos de registro de eventos o logs.

c) Buzones de los usuarios de correo.

d) Archivos de configuración personales de los usuarios depositados en el servidor.

La frecuencia y el número de copias de seguridad efectuadas podrán variar en función de la disponibilidad y características de los datos a almacenar y de la gestión del servicio.

El usuario será responsable de efectuar copia de los mensajes que considere importantes en un medio local y personal.

6.10 Derechos de los usuarios

En relación con los derechos de los usuarios será de aplicación lo previsto en el apartado 1 de la Norma de Uso de los Recursos y Sistemas de Información de la UEx.

Sin perjuicio de lo anterior, los usuarios del servicio de correo electrónico corporativo tienen derecho a:

a) Ser informados a través del correo electrónico y de la página web institucional de cualquier cambio en el servicio que les afecte.

b) Ser informados permanentemente del estado de funcionamiento del servicio de correo.

c) Ser atendido por el Centro de Atención al Usuario (CAU) en relación con las dudas, incidentes o problemas que surjan durante el uso del servicio de correo y obtener una respuesta o solución a las peticiones; así como, ser informado sobre incidentes y problemas que puedan existir con su cuenta de correo.

d) Recibir las comunicaciones y avisos de caducidad de cuentas descritos anteriormente.

e) Solicitar, según lo indicado anteriormente, a través del CAU la recuperación de mensajes y de carpetas borradas de sus buzones de correo.

f) Solicitar información acerca del uso de sus cuentas de correo.

6.11 Obligaciones de los usuarios

Acerca de las obligaciones de los usuarios será de aplicación lo previsto en la Norma de Uso de los Recursos y Sistemas de Información de la UEx.

Sin perjuicio de lo anterior, los usuarios de cuentas de correo electrónico corporativo de la UEx quedan obligados a:

a) Responsabilizarse de todas las actividades realizadas mediante el empleo de la cuenta de correo personal que tengan asignada o en el marco de una cuenta de correo de grupo para cuyo empleo estén autorizados.

b) No delegar el uso de su cuenta de correo personal a nadie y mantener en secreto, por tanto, las credenciales de acceso al mismo.

c) Avisar al Centro de Atención de Usuarios (CAU) de cualquier comportamiento anómalo que detecten en el uso de sus cuentas de correo.

6.12 Documentación y notificación de incidencias

La documentación, instrucciones, recomendaciones y resto de información que deba hallarse públicamente disponible en relación con el servicio de correo electrónico corporativo se mantendrá actualizada por el SICUE en la web institucional, en el apartado correspondiente a Normas: https://www.unex.es/

De la misma manera que con otros servicios electrónicos prestados por la UEx, todas las incidencias, dudas, avisos y cualquier comentario relacionado con el servicio de correo electrónico de la UEx se podrán dirigir al CAU.

6.13 Uso adecuado y seguro del correo

A continuación, se incluye un conjunto de normas que tienen como objetivo reducir el riesgo en el uso del correo electrónico.

El uso inapropiado o el abuso en el servicio de correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio.

La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras no vuelva a ser activada.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, el SICUE podrá cambiar la contraseña de una cuenta (o cualquier otro mecanismo de autenticación que se esté utilizando). Esto podría impedir al usuario el acceso al resto de los servicios basados en las dichas credenciales.

Normas:

- **Utilizar el correo electrónico exclusivamente para propósitos profesionales.** Gran parte de los mensajes de correo electrónico no deseados que lleguen a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.

  Existen numerosos proveedores de servicios de Internet que proporcionan cuentas de correo electrónico gratuitas (gmail, yahoo, hotmail, etc.) que los usuarios pueden configurar y usar en sus ordenadores privados, fuera de las dependencias de la UEx y de su perímetro de seguridad.

- **Usar contraseñas seguras.** Para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es conveniente utilizar contraseñas robustas. Dada la importancia de la gestión de contraseñas, se va a desarrollar una norma específica: **NP.40 Normas de Creación y uso de contraseñas**.

- **No ceder el uso de las cuentas de correo.** Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales - para los que deberá solicitarse y obtenerse la correspondiente autorización -, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial.

  Además de ello, es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios.

- **Revisar la barra de direcciones antes de enviar un mensaje.** El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo Con Copia (CC). Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.

- **No se deben enviar o reenviar correos de forma masiva.** Si se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.

- **No enviar mensajes en cadena.** Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe notificar la incidencia.

- **No responder a mensajes de Spam.** La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la UEx.

  En cualquier caso, nunca debe responderse a los mismos.

- **Utilizar mecanismos de cifrado de la información.** Los mensajes que contengan información sensible, confidencial o protegida deben cifrarse. El Servicio de Informática y Comunicaciones de la UEx (SICUE) pondrá a disposición de los usuarios que lo precisen el acceso a la aplicación necesaria para el cifrado de información.

- **Asegurar la identidad del remitente antes de abrir un mensaje.** Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) del usuario atacado. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información sensible, confidencial o protegida a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse.

  Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

- **Desactivar la vista previa.** Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.

- **Limitar el uso de HTML.** El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.

- **Utilizar herramientas de análisis contra código dañino.** La utilización de herramientas tales como antivirus y cortafuegos ayuda a detectar el código malicioso y a mitigar sus efectos. Por ello, debe configurarse el antivirus con la opción de analizar el correo electrónico entrante.

- **No abrir correos basura ni correos sospechosos.** Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportar se el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.

- **No ejecutar archivos adjuntos sospechosos.** No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso.

  Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (PDF, Word, Excel, etc.).

- **Informar de correos con virus, sin reenviarlos.** Si el usuario detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad y no reenviarlo, para evitar su posible propagación.
- **No utilizar el correo electrónico como espacio de almacenamiento.** La capacidad de espacio en los servidores de correo de la UEx es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos.
- En relación con el **acceso remoto (vía web)** al correo electrónico, deben adoptarse las siguientes cautelas:
    - Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
    - Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
    - Desactivar la interpretación de contenidos remotos a la hora de leer mensajes de correo vía webmail.
    - Desactivar las características de recordar contraseñas para el navegador.
    - Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
    - Salvo autorización expresa, está prohibida la instalación de *addons* para el navegador.
    - Además de lo anterior, cualquier información sensible, confidencial o protegida que permanezca almacenada en el servidor de correo podría ser accedida por un atacante, lo que aconseja su borrado.

7 Prevención contra SPAM

El término spam se define como el envío de correos no solicitados, de forma masiva, a direcciones de correo electrónico, constituyendo uno de los problemas de seguridad más habituales con los que se enfrentan las organizaciones. Tales mensajes pueden contener código dañino que, de penetrar en los sistemas de información, podrían llegar a colonizar una institución y propagarse a través de las redes de comunicaciones.

Además de las medidas técnicas de prevención y eliminación de spam ya instaladas en la UEx, se detallan seguidamente las normas que todo usuario deberá seguir para hacer frente a este problema:

- Con carácter general, sólo se proporcionará la dirección de correo electrónico profesional de la UEx a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo de la UEx en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza. Muchos ataques de spam se sirven de estas direcciones, introducidas en sitios no seguros.
- Con carácter general, si no se conoce el remitente de un correo, y/o el asunto de este es extraño, se recomienda borrar el mensaje (o situarlo en cuarentena hasta disponer de más datos), especialmente si contiene ficheros adjuntos.

La UEx dispone de sistemas *antispam* para la detección y borrado de mensajes identificados como spam. Sin embargo, es posible que dichos sistemas no puedan eliminar la totalidad de estos mensajes. Por este motivo, si el usuario recibe un mensaje de spam, deberá:

- Si lo reconociera como tal por la dirección o el asunto que contiene, lo borrará inmediatamente (sin abrirlo).
- No responderá nunca.
- No accederá a los enlaces o anexos que pudieran contener.
- Comunicarlo inmediatamente al SICUE, abriendo una incidencia en el CAU: https://cau.unex.es/.

8 Modelo de aceptación y compromiso de cumplimiento

Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la UEx deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

La presentación para su conocimiento, comprensión y aceptación de esta norma a los usuarios del correo electrónico se realizará de forma electrónica usando la aplicación de gestión de credenciales.

9 Referencias

Esta Norma se apoya y se ve complementada por las siguientes referencias:

Internas:

- PO.01 Política de Seguridad de la Información de la Universidad de Extremadura. D.O.E. 109/2023, de 8 de junio.
- NG.01 Normativa General De Utilización De Los Recursos Y Sistemas De Información.
- NP.40 Normas de Creación y uso de contraseñas.

Externas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Guía de seguridad de las TIC CCN-STIC 821 Anexo III. Normas de uso del correo electrónico (e-mail) NP20.

Apéndice: Lenguaje de género

En coherencia con el valor de la igualdad de género asumido por la Universidad de Extremadura, todas las denominaciones que en esta Norma se efectúan en género masculino, cuando no hayan sido sustituidas por términos genéricos, se entenderán hechas indistintamente en género femenino.