Manual de buen uso del correo electrónico

Guía para las personas trabajadoras para la protección de la privacidad en el uso del correo electrónico

apdcat
Autoritat Catalana de Protecció de Dades

Generalitat de Catalunya

Indice

Tutorial anexo

Cómo firmar y cifrar un mensaje de correo electrónico

Correo electrónico

☐ DEFINICIONES

Correo electrónico:	sistema de mensajería que permite la transmisión de mensajes entre usuarios, sin necesidad que estén conectados al mismo tiempo.
Dirección de correo:	conjunto de palabras o signos que identifican el emisor o el receptor de un mensaje de correo electrónico.
Usuario:	persona que utiliza los medios informáticos, en este caso el correo electrónico.
Cuenta de correo o buzón de correo:	espacio facilitado por un proveedor de correo electrónico, donde se envían, reciben o almacenan los mensajes de correo electrónico.
Proveedor de correo:	empresa que ofrece el servicio de correo electrónico. El proveedor asigna una dirección de correo, a la cual se puede acceder mediante un nombre de usuario y una contraseña.
Dirección IP:	número que permite identificar los dispositivos dentro de una red que utiliza el protocolo IP, como Internet.
Empresa:	en esta Guía, se utiliza el término *empresa* para referirse a todas las entidades incluidas dentro del ámbito de actuación de la APDCAT.

¿Qué es una dirección de correo electrónico?

Es el conjunto de palabras o signos que identifican un buzón en el cual o desde el cual se envían mensajes de correo electrónico. Se elabora a partir de un conjunto de signos o palabras libremente escogidos:

Nombre de usuario
Identifica el buzón de correo electrónico

@ Arroba
Podemos reconocer fácilmente una dirección de correo ya que siempre tiene la @

Dominio
Identificación que facilita el proveedor del servicio de correo electrónico

jordi @ llibreters.cat

¿La dirección de correo electrónico es un dato de carácter personal?

Es dato personal

☐ Direcciones personalizadas

La dirección de correo electrónico identifica directamente a la persona titular de la cuenta (con el nombre y los apellidos, las iniciales, el cargo, un número identificativo, etc.) y, por lo tanto, se tiene que considerar como dato de carácter personal.

joanidentitat@gencat.cat
E.C@gencat.cat
Directora@gencat.cat
000000000857346@gencat.cat

¡Atención!

Que una dirección sea personalizada no quiere decir que el correo se pueda utilizar para finalidades privadas. Hay que consultar las normas de uso del correo corporativo, para conocer si está permitida la utilización con fines personales.

☐ Direcciones no personalizadas

En este caso, la dirección de correo no identifica directamente a la persona titular de la cuenta de correo:

Akatombe80@gmail.com
Abc123@terra.net

Aunque la dirección por sí sola no identifica a la persona titular de la misma (utiliza una combinación alfanumérica abstracta o sin ningún significado), ésta puede ser fácilmente identificable.

- porque la dirección puede aparecer junto con otros datos que permiten la identificación.
- por el contenido del mensaje.
- a través de los datos de que dispone el servidor de correo, sin un esfuerzo desproporcionado.

No es dato personal

☐ Direcciones genéricas

La dirección de correo electrónico responde, por ejemplo, a un servicio, una actividad o un área de la organización:

consultes@gencat.cat

En estos casos, la información que nos ofrece la dirección de correo electrónico no se puede vincular a una persona física identificada o identificable. Por lo tanto, no se puede considerar como dato de carácter personal. A menudo la pueden atender usuarios diferentes, previamente determinados.

¡Atención!

En las cuentas vinculadas a estas direcciones, ni el trabajador ni las personas que se relacionan con ella pueden tener ninguna expectativa de privacidad.

☐ ¿Pueden publicar mi dirección de correo profesional en la web corporativa de mi empresa, sin mi consentimiento?

Sí, con finalidades estrictamente profesionales y sólo en los casos en que resulte necesario, de acuerdo con las funciones que tenga atribuidas el trabajador. En caso contrario, la dirección se podrá publicar sólo en la intranet.

¿Qué sistemas de correo electrónico podemos utilizar?

El correo electrónico es un servicio de mensajería interpersonal que permite la transmisión de mensajes entre usuarios sin necesidad que estén conectados al mismo tiempo. Hay diferentes aplicaciones que gestionan sistemas de correo electrónico, que se pueden agrupar, básicamente, en dos modalidades:

☐ Cliente de correo electrónico

- Son programas que sirven para gestionar los mensajes recibidos y para escribir nuevos mensajes (p. ej. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.).
- El programa descarga todos los mensajes que se almacenan en el ordenador, sin perjuicio que determinados protocolos (caso de IMAP) puedan mantenerlos en el servidor.
- Se puede instalar en diferentes dispositivos (ordenador fijo, portátil, teléfono inteligente o *smartphone*, tableta, etc ...).

Thunderbird reclaim your inbox. Outlook

☐ Webmail o correo web

- Con independencia de que se pueda acceder a éste también a través de un cliente de correo, se trata de un sistema de acceso a un servicio de correo electrónico utilizando el navegador de Internet y el protocolo http o https.
- Permite recibir y enviar correos desde cualquier lugar, a través de una web.
- Los mensajes se almacenan en el servidor donde se aloja la cuenta de correo web.

Windows Live Hotmail · Gmail by Google · msn · YAHOO!

¡Atención! **Los servidores de correo pueden estar en terceros países**, que quizás no cuentan con un nivel adecuado de protección de los datos de carácter personal, y a menudo, especialmente en el web mail, las condiciones las fija y las modifica unilateralmente el proveedor.

Cuando se trate de servicios ofrecidos gratuitamente, recordad que:

- Estas condiciones acostumbran a incluir la autorización para el tratamiento de la información que se contiene en ellas con finalidades publicitarias u otras finalidades.
- A menudo los servidores realizan un análisis automático del contenido de los mensajes enviados o recibidos. Este análisis del contenido de los mensajes puede ser útil, por ejemplo para detectar virus. Pero, además, a menudo los proveedores lo utilizan para ofrecer, en la misma aplicación de correo, anuncios relacionados con el mensaje de correo electrónico o de otras circunstancias relacionadas con su envío.

☐ ¿Puedo utilizar el correo con finalidades privadas?

- En los supuestos en que las normas de uso del correo establecidas por la empresa admitan un cierto uso privado, no hagáis un uso abusivo de ellas.
- No facilitéis la dirección de correo profesional en trámites personales.
- Haced constar en el título de los mensajes la naturaleza privada o personal del mensaje o alguna otra expresión que permita a la empresa deducir este carácter, en caso de que ésta tenga que acceder a la cuenta de correo.
- Eliminad, tan pronto como sea posible, la información privada almacenada en las cuentas de correo facilitadas por la empresa. Especialmente, cuando os ausentéis de vuestro puesto de trabajo por un período largo (vacaciones, viajes, ingresos hospitalarios, etc.).
- Si sois representantes sindicales en vuestra empresa, podéis usarlo para difundir información sindical al resto de trabajadores, siempre que no se perturbe la actividad normal de la empresa.

☐ ¿La empresa puede acceder a mi correo electrónico?

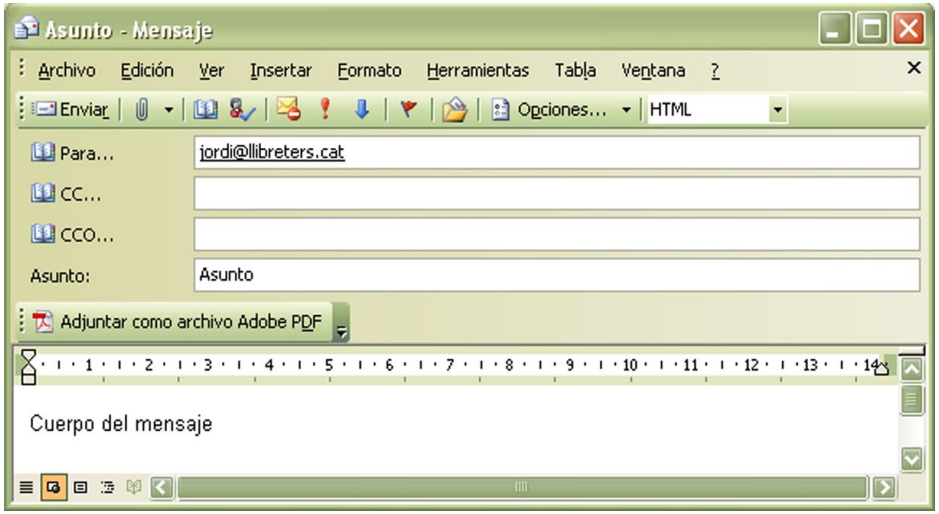
La empresa sólo puede acceder a las cuentas de correo electrónico corporativo facilitadas a sus trabajadores cuando este acceso esté justificado y no haya ningún otro mecanismo que permita alcanzar el objetivo perseguido sin necesidad de acceder a él.

Este acceso se tiene que llevar a cabo de acuerdo con las normas de uso del correo electrónico aprobadas previamente por la empresa, que tienen que advertir sobre los mecanismos de control del uso de las tecnologías que puedan afectar la privacidad de las personas y las consecuencias que se pueden derivar del mal uso.

Recordad

- Consultar las normas de uso del correo electrónico corporativo para conocer:
  - Si se admite el uso del correo profesional asignado para finalidades privadas.
  - Si la empresa facilitará a los trabajadores una cuenta de correo para uso privado.
  - Si la empresa permite a los trabajadores utilizar una cuenta de correo del propio trabajador durante el horario laboral para finalidades privadas.
- Hay que evitar el uso de cuentas de correo para comunicaciones relacionadas con la actividad propia de la empresa, que no hayan sido proporcionadas por proveedores designados por la empresa.

¿Qué elementos forman un correo electrónico?



☐ Dirección de correo del emisor y del destinatario

A menudo, la dirección de correo se puede vincular fácilmente a una persona física. En ocasiones, la misma dirección ya facilita la identificación. En otras, en el campo correspondiente a la dirección, junto con ella, o incluso sustituyéndola, aparece la identificación de la persona que es titular.

☐ Asunto

Conviene que el asunto describa de forma concisa la naturaleza o el contenido del mensaje y, si es posible, se evite incluir en él datos de carácter personal.

El grado de confidencialidad de los datos que se incluyan en el asunto será menor que el de la información que contiene el cuerpo del mensaje, dado que la simple visualización de la bandeja de entrada o salida permite leer el asunto.

☐ Fecha y hora del correo

La fecha y la hora del correo también pueden constituir un dato personal, dado que permiten establecer el momento en que se envía e, incluso, pueden llegar a permitir establecer el lugar donde estaba una persona.

☐ Cuerpo del mensaje

Es el contenido del mensaje. Puede consistir en un texto, con formato o sin, o en imágenes, que pueden contener datos de carácter personal. También puede contener enlaces a páginas web o documentos que contengan datos personales.

☐ Pie de firma

Es el texto que aparece bajo la identificación de quien suscribe el mensaje. Normalmente, ofrece información sobre el cargo y la organización a la cual pertenece el emisor.

A menudo, los sistemas de correo electrónico ofrecen la posibilidad de incorporar, en los mensajes de correo, un pie de firma de forma automática.

☐ Documentos adjuntos

El correo electrónico permite adjuntar al mensaje imágenes, documentos, vídeos o audio. El volumen de información personal que pueden incluir los documentos adjuntos puede ser muy grande.

Recordad

- Si se trata de un mensaje de naturaleza privada, y ello no se puede deducir del encabezamiento, conviene indicarlo en el asunto.
- Evitad incluir en el asunto información personal, a menos que resulte estrictamente necesario.
- Verificad el contenido del correo electrónico, especialmente de los ficheros adjuntos, antes de enviarlo, para comprobar la identidad de las personas destinatarias, si los datos que figuran en él se pueden transmitir y cuáles son las medidas de seguridad exigibles.
- Evitad la comunicación de datos identificativos innecesarios, cuando el contenido haga referencia a terceras personas. En caso de que no se pueda evitar la comunicación de estos datos, se recomienda hacerlo mediante un archivo adjunto.
- Inhabilitad la opción de pie de firma automático o, si procede, eliminad del pie de firma la información relativa al cargo y la organización donde se presta los servicios, cuando se trate de mensajes de correo para finalidades privadas.

Acceso al correo: identificación y autenticación

La empresa tiene que establecer, en las normas de uso del correo electrónico, una política de contraseñas adecuada para garantizar la identificación inequívoca y personalizada de cualquier usuario.

☐ Identificación

Procedimiento para conocer la identidad de un usuario, en este caso del usuario de correo electrónico. Se asigna a cada usuario un nombre con esta finalidad.

☐ Autenticación

Procedimiento de comprobación de la identidad de un usuario. En un sistema de correo, se hace normalmente a través de la introducción de una contraseña o password además de la identificación del usuario, aunque también se pueden utilizar otros sistemas, como un certificado digital.

☐ Contraseña

Información confidencial constituida por una cadena de caracteres.
La robustez de la contraseña depende de las características exigidas para establecerla (política de contraseñas).

Una **contraseña** se puede considerar **fuerte** si:

- Tiene una longitud mínima de 8 caracteres.
- Se ha escogido al azar y no se puede encontrar en ningún diccionario.
- Sólo la puede deducir el mismo usuario.
- Requiere esfuerzos desproporcionados averiguarla.
- Incluye letras, números, mayúsculas y minúsculas y, si lo permite el sistema, símbolos.

Una **contraseña** se puede considerar **débil** si:

- Identifica fácilmente al usuario.
- Contiene menos de 8 caracteres.
- Viene predeterminada por el sistema o por el administrador del sistema.
- Es fácilmente identificable utilizando diccionarios o bien consiste en nombres propios, fechas significativas, números conocidos o variaciones simples de estas palabras.

Recordad

- Modificad la contraseña predeterminada por el sistema, cuando accedáis a él por primera vez.
- Escoged contraseñas fuertes. Una clave personal de acceso que sea difícil de descifrar es garantía de seguridad.
- Guardad la contraseña de forma segura. No la guardéis anotada en lugares de fácil acceso.
- Cambiad la contraseña con la periodicidad requerida por el sistema.
- Para los casos de olvido de la contraseña, cuando se tenga que responder una pregunta para recuperarla o modificarla, evitad preguntas que se puedan responder con una mínima investigación.
- Comunicad inmediatamente, siguiendo el procedimiento de gestión de incidencias establecido, cualquier incidencia que comprometa la seguridad.
- No facilitéis la contraseña a terceras personas, aunque os la soliciten para hacer pruebas al sistema o similares.
- No escojáis la opción de recordar la contraseña.
- Cerrad la sesión del correo electrónico o bloquead el ordenador, cuando abandonéis, aunque sea puntualmente, el puesto de trabajo (p. ej. con las teclas Ctrl+Alt+Supr).

Buenas prácticas

En el momento de utilizar el sistema de correo electrónico profesional, tenemos que respetar la legislación vigente y lo que se establece en las Normas de uso del correo electrónico establecidas por la empresa. Más allá de esta cuestión, conviene tener presentes algunas buenas prácticas para utilizar esta herramienta de una forma respetuosa con la privacidad de las personas.

Cuando queremos escribir a más de un destinatario ...

- Antes de contestar un correo que se ha enviado a diversas personas, hay que valorar la necesidad de enviar la respuesta sólo al remitente o también al resto.
- La opción de responder a todo el mundo hará visible vuestro mensaje a todas las personas que aparecían en él como destinatarias.

¿Y si queremos reenviar el correo?

- Utilizad la opción de reenviar sólo en aquellos casos en qué tanto el emisor como el contenido del mensaje, y toda la información de la cadena de correos que forman parte de él, puedan ser accesibles para la persona destinataria.
- Evitad el envío de mensajes piramidales o en cadena, para evitar dar a conocer indebidamente direcciones de correo o contenidos a terceras personas y para evitar la propagación de virus o software malicioso *(malware)*.

¿Qué es la copia oculta (CCO)?

La opción CCO (copia de carbón oculta) o C/o (Copia oculta) permite que, en correos dirigidos a una pluralidad de personas destinatarias, sus direcciones o su identificación permanezcan ocultas para el resto de personas destinatarias.

Recordad

Para evitar la divulgación del resto de direcciones de las personas destinatarias del correo electrónico, utilizad la opción CCO cuando no dispongáis de su consentimiento o cuando no concurra alguna otra circunstancia que permita revelar este dato.

Con la utilización de esta opción, no sólo se preserva la confidencialidad del resto de personas destinatarias sino que también se evitan prácticas de correo basura *(spam)* o similares.

Hay que tener en cuenta, sin embargo, que en algunos casos el filtro antiinundación *(antispam)* puede identificar erróneamente este tipo de mensajes, y clasificarlos como correo basura.

¿Se pueden adjuntar documentos al correo electrónico?

Hay que consultar las normas de uso del correo corporativo, para conocer cuáles son las comunicaciones de datos que se pueden hacer mediante el correo electrónico y, si procede, con ficheros adjuntos, quién está autorizado a realizarlas, y cómo se tiene que tratar la información que se reciba por esta vía.

Recordad

Analizad, antes de enviar un fichero por correo, si contiene datos personales. Si es así:

- Aseguraros de que todas las personas a quienes habéis dirigido el correo pueden acceder a esta información, de acuerdo con sus funciones. Si no fuera así, no enviéis este correo. En caso de que fuera necesario enviarlo, seleccionad la información que corresponda a cada una de las personas destinatarias.
- Utilizad técnicas de cifrado de documentos, en el caso de los datos que requieren un nivel alto de seguridad de acuerdo con el RLOPD. Recordad que los correos electrónicos y los documentos que se adjuntan a ellos tienen la consideración de soportes, a efectos de las medidas de seguridad a aplicar establecidas en el RLOPD.

¿Cómo podemos garantizar nuestra identidad y la autenticidad del contenido de nuestros correos electrónicos?

Para garantizar la autenticidad y la integridad de las comunicaciones, podemos utilizar la firma electrónica mediante el certificado facilitado por la empresa, de acuerdo con las condiciones de uso que se establezcan en las normas de uso del correo electrónico:

☐ Firma electrónica

Conjunto de datos en forma electrónica que, consignados y/o asociados con otros, se pueden utilizar como medio de identificación de la persona que firma, mediante un sistema de criptografía asimétrica. Este mecanismo permite autenticar el emisor y la integridad del mensaje.

Se puede generar a partir de un certificado electrónico.

La empresa, con la colaboración, si procede, de la Agencia Catalana de Certificación, tiene que proveer a su personal de sistemas de firma electrónica que puedan identificar de forma conjunta al titular del puesto de trabajo o cargo y a la administración o empresa donde presta servicios.

Podéis consultar los pasos para **firmar electrónicamente un correo electrónico** en el siguiente enlace:

Para garantizar su confidencialidad, podemos utilizar el cifrado:

☐ Cifrado

El cifrado transforma el mensaje, utilizando una clave, para evitar que quien no la conozca lo pueda interpretar. El cifrado garantiza que la información no sea inteligible ni manipulada por terceros.

La normativa de protección de datos impone el cifrado en la transmisión de datos de carácter personal a través de redes públicas o redes sin hilo de comunicaciones electrónicas, cuando el tratamiento requiere la aplicación de medidas de seguridad de nivel alto:

- Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Datos obtenidos con fines policiales sin el consentimiento de las personas afectadas.
- Datos derivados de actos de violencia de género.

Para descifrar un mensaje, hace falta tener instalado un programa de cifrado y conocer la clave que permite descifrarlo.

Podéis consultar los pasos para **cifrar un correo electrónico** en el siguiente enlace:

¿Cómo sabemos que se ha recibido nuestro mensaje?

Un error en la identificación del destinatario o en la transcripción de la dirección puede comportar que el mensaje sea recibido por una persona diferente a la prevista. En este caso, la confidencialidad del contenido del correo electrónico se ve comprometida.

Normalmente, los sistemas de correo permiten activar la opción de confirmación de entrega o de confirmación de lectura. Estas opciones ofrecen más seguridad, dado que permiten conocer el éxito del envío. Pero hay que comprobar, además, mediante la identificación que aparece en el mensaje de respuesta, que el mensaje lo ha recibido la persona a la cual iba destinado. Sin embargo, hay que tener en cuenta que el destinatario puede no autorizar que se envíe la confirmación de entrega o de lectura.

Recordad

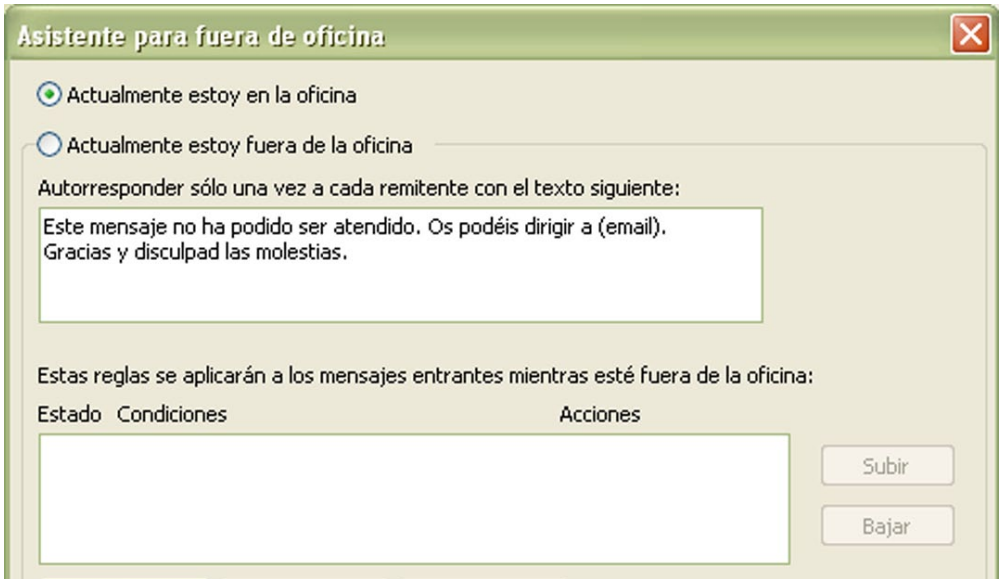
- Comprobad la dirección del destinatario, antes de enviar el correo. Si el mensaje va dirigido a un grupo de usuarios previamente configurado, se recomienda utilizar listas de distribución (si el programa lo permite).
- Utilizad, siempre que sea posible, la opción de copiar y pegar en lugar de teclear las direcciones. Así, evitaréis los errores que se pueden producir al reescribirlas.
- Asegurad que los destinatarios son los correctos, cuando los seleccionéis del directorio corporativo de direcciones, mediante la comprobación de alguna otra de las informaciones que aparece en el directorio.
- Cuando el programa complete automáticamente la dirección que estáis introduciendo mediante el teclado, si la dirección no os resulta conocida comprobad la corrección consultando las propiedades del contacto.
- Activad la opción de confirmación de entrega y/o confirmación de lectura por parte del destinatario, antes de enviar un mensaje, y comprobad que el destinatario previsto ha recibido el mensaje.
- Podéis incluir, en el pie del mensaje, algún texto preestablecido que recuerde la necesidad de destruir el mensaje, en caso de que haya sido recibido por error, como también la conveniencia de ponerlo en conocimiento del remitente. El texto podría ser similar al siguiente:

  "AVISO

  Este mensaje puede contener información confidencial y está dirigido únicamente a su destinatario. Si lo habéis recibido por error, no lo divulguéis a terceras personas, notificadlo al remitente y borradlo de vuestro sistema. Muchas gracias."

¿Durante nuestra ausencia, quién puede contestar los correos?

En supuestos de ausencia programada, y con la finalidad de dar respuesta a los correos electrónicos entrantes, se puede activar la función del mensaje de respuesta automática "Fuera de oficina".



☐ Hay que tener en cuenta que:

- El mensaje de ausencia de oficina permite, a personas que lleven a cabo acciones de envío masivo de correo basura, validar vuestra dirección como una dirección realmente existente.
- Según cuál sea el contenido del mensaje de respuesta, quizás estáis dando un exceso de información a la persona que lo reciba.
- Al dar información sobre vuestra ausencia, un tercero puede utilizar esta información para hacer un envío masivo de correos electrónicos a vuestro buzón, con la finalidad de bloquearlo.
- En casos de ausencia, cuando la continuidad del servicio requiera redireccionar el correo a la dirección de otro trabajador, si las normas internas de uso del correo permitan un cierto uso privado, conviene advertir de esta circunstancia a vuestros contactos personales.

¿Y si queremos acceder al correo desde fuera de nuestra oficina?

☐ Acceso remoto

Si la empresa lo autoriza, el acceso al correo electrónico se podrá hacer a través de sistemas remotos de acceso, mediante dispositivos de la empresa o dispositivos personales del trabajador o de terceras personas, y también por medio de dispositivos móviles, como ordenadores portátiles, teléfonos inteligentes o *smartphones*, tabletas, etc.

Recordad

Cuando para acceder al correo electrónico vía web mail se utilicen ordenadores de uso compartido:

- Utilizad sólo protocolos seguros, como el htpps.
- Borrad el rastro de vuestra navegación.
- Cerrad la sesión cada vez que salgáis de ella.
- No escojáis la opción de recordar la contraseña que se ofrece a veces, para evitar que quede registrada en aquel ordenador.

☐ Acceso mediante dispositivos móviles

Los dispositivos móviles tienen que contar con las mismas medidas de seguridad que los puestos de trabajo fijos, pero la utilización de este tipo de acceso al correo genera nuevos riesgos que hay que prevenir.

Recordad

- Cumplid las políticas corporativas de seguridad relativas al uso de usuarios y contraseñas.
- Evitad el uso de redes Wi-Fi que no ofrezcan confianza.
- Instalad en estos dispositivos sólo las aplicaciones autorizadas previamente por el responsable de seguridad o la persona a quien corresponda.
- No almacenéis información sensible en local en estos dispositivos.
- En caso de robo o pérdida, avisad inmediatamente al responsable de seguridad de la empresa o la persona a quien corresponda.
- Algunos dispositivos pueden configurarse para que el usuario o, si procede, el servidor de correo, puedan bloquearlos remotamente o localizarlos en caso de pérdida o robo.

Correo basura o *Spam*: ¿Cómo evitarlo?

Hay que tener en cuenta que, las comunicaciones publicitarias o promocionales por correo electrónico las tienen que haber pedido o autorizado expresamente las personas destinatarias, a menos que se cumplan las condiciones siguientes:

- Haya una relación contractual previa, que esté vinculada a la misma,
- La dirección se haya obtenido de forma lícita y
- La comunicación se refiera a productos o servicios de la misma empresa, similares a los que habían sido contratados.

Recordad

- Evitad responder correos identificados como correo basura *(spam)* o de procedencia dudosa. Ello validaría la dirección de correo como existente y probablemente generaría el envío de más correo basura.
- No hagáis clic sobre los anuncios que aparezcan en los mensajes de correo susceptibles de ser spam.
- No abráis ficheros adjuntos de mensajes con emisores desconocidos, sin haberlos analizado antes con un programa antivirus.
- No activéis la opción de vista previa.
- Vigilad a quién facilitáis la dirección de correo electrónico.
- Evitad participar en los correos electrónicos en cadena.
- Enviad mensajes con copia oculta.
- Borrad las direcciones del mensaje anterior cuando reenviéis un correo electrónico.
- No publiquéis la dirección de correo electrónico en buscadores, foros, direcciones de contacto o páginas web, a menos que sea estrictamente necesario.
- Instalad filtros automáticos antiinundación o *anti-spam* o de control del correo no deseado.
- Utilizad programas antivirus y que detecten software malicioso *(malware)*.
- Leed atentamente las políticas de privacidad y las condiciones de cancelación cuando, en ejercicio de vuestras funciones, contratéis un producto o servicio o hagáis una suscripción en línea.

Otras medidas de seguridad ...

Recordad

- Adaptad las opciones de seguridad de vuestro correo a la naturaleza de los datos que preveáis recibir o comunicar.
- Situad y orientad las pantallas de los terminales de manera que se preserve el contenido de los mensajes respecto de terceras personas que se puedan encontrar en las dependencias donde se encuentra vuestro puesto de trabajo.
- No instaléis software no autorizado por la empresa.
- Programad la eliminación, de forma inmediata, de los mensajes que puedan contener virus o *malware*. El borrado completo requiere eliminarlos, también, de la papelera de reciclaje.
- Comunicad al área encargada de la seguridad de la información cualquier incidencia que se detecte en el sistema, de acuerdo con el protocolo que establezca la empresa.