MADRID

INFORMÁTICA DEL AYUNTAMIENTO DE MADRID

INSTRUCCIÓN SOBRE USO SEGURO DEL CORREO CORPORATIVO

[ ] versión 1 12/03/2019

Uso interno del Ayuntamiento de Madrid

CUADRO DE CONTROL			
Código	[ ]	**Estado**	Final
Título	Instrucción sobre uso seguro del correo corporativo		
Autor	Arquitectura y Seguridad (IAM)		
Versión	1	**Fecha de versión**	12/03/2019
Difusión	Uso interno -		

CONTROL DE CAMBIOS			
V.	**Fecha**	**Autor/es**	**Descripción**
1	27/2/19	Arquitectura y Seguridad (IAM)	Versión inicial
1	12/03/19		Aprobación Comité Municipal Seguridad de la Información del Ayto y sus OOPP

Índice

1 INTRODUCCIÓN

El correo electrónico es una de las herramientas más utilizadas en cualquier entorno corporativo para el intercambio de información. A pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros, el correo electrónico sigue siendo la herramienta más utilizada para enviar y recibir mensajes y ficheros adjuntos de manera rápida y eficaz.

Mediante Decreto de 18 de febrero de 2013 de la Delegada de Gobierno de Economía, Hacienda y Administración Pública se estableció el correo electrónico como medio de comunicación entre las Unidades del Ayuntamiento y con los ciudadanos.

El Acuerdo de 24 de julio de 2018 del Pleno del Ayuntamiento de Madrid por el que se aprueba la modificación del Reglamento de Ordenación del Personal del Ayuntamiento de Madrid enfatiza la obligación de conservar y preservar la privacidad de los sistemas de identificación y firma en el uso de medios electrónicos (Art. 23.3), siendo el correo electrónico uno de los medios electrónicos para comunicación interna (Art. 24). El artículo 26.2 reitera la imposición de confidencialidad en la custodia de la contraseña del correo electrónico, que ha de permitir garantizar la identidad del remitente y del destinatario, así como la confidencialidad del contenido del mensaje y la determinación de las fechas de su envío y recepción.

Este documento se ha elaborado conforme a lo dispuesto en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad y su posterior modificación mediante Real Decreto 951/2015.

Este documento forma parte del esquema normativo del Ayuntamiento de Madrid y sus Organismos Públicos (en adelante “Ayuntamiento”) en lo referente a la Seguridad de la Información, en el que el primer nivel lo constituye la Política de Seguridad de la Información del Ayuntamiento (PSI) y el segundo nivel –al que pertenece este documento- desarrolla dicha política mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información.

Este documento se considera de uso interno del Ayuntamiento de Madrid y, por tanto, no podrá ser divulgado salvo autorización del responsable de seguridad del Ayuntamiento.

2 OBJETO Y ÁMBITO DE APLICACIÓN

Esta instrucción es de aplicación a todo el ámbito de actuación del Ayuntamiento conforme a lo definido en la PSI.

El Organismo Autónomo Informática del Ayuntamiento de Madrid (IAM) ha elaborado este documento cuyo objetivo es difundir una serie de instrucciones y recomendaciones para asegurar que el servicio de correo electrónico que el Ayuntamiento de Madrid y sus OOPP, a través de IAM, proporciona como recurso fundamental en el desarrollo de la actividad municipal, sea utilizado de forma segura, eficaz y eficiente.

3 APROBACIÓN

Esta instrucción ha sido validada por el Comité Municipal de Seguridad de la Información (CMSI) y entrará en vigor cuando sea aprobada por la persona titular de la Gerencia de la Ciudad, órgano competente en materia de tecnologías de la información y comunicaciones municipales.

4 DESCRIPCIÓN DEL SERVICIO

4.1 Tipos de cuentas de correo electrónico

i. Cuentas personales

Las cuentas de correo personales, también denominadas individuales, son las asignadas a una persona concreta para el desempeño de las labores encomendadas en el ámbito municipal. Se crean y suprimen mediante procesos automáticos cuando el personal municipal causa alta o baja en el Ayuntamiento o sus OOPP.

Estas cuentas están destinadas para un uso profesional y no particular.

Todo el personal del Ayuntamiento de Madrid y sus OOPP dispondrá de un buzón y una dirección de correo electrónico (comúnmente conocida como “cuenta de correo”). Esta cuenta está asignada de forma individual e identifica a cada persona que trabaja en el Ayuntamiento de Madrid y sus OOPP, que es responsable de su correcta utilización.

En caso de que un empleado o empleada municipal deje de serlo, el interesado o interesada podrá, con una semana de antelación a su desvinculación municipal, solicitar, a través del procedimiento existente, que su cuenta de correo xxxx@madrid.es sea redirigida a otra cuenta de correo personal o profesional, o que la cuenta xxxx@madrid.es sea mantenida activa durante quince días. En caso de no solicitarlo, la cuenta se dará de baja según el proceso automático existente.

ii. Cuentas genéricas

Las cuentas genéricas no están vinculadas a una persona física concreta, pueden ser utilizadas por una o varias personas y se utilizan para identificar determinados servicios.

Las unidades organizativas podrán disponer de tantos buzones de correo genéricos como sea necesario para el desarrollo de sus funciones o la identificación de los servicios. Estas cuentas han de tener necesariamente una persona responsable designada, que deberá ser un empleado o empleada del Ayuntamiento de Madrid o de sus OOPP.

Las cuentas de correo genéricas, al igual que las personales, están destinadas para un uso profesional en el ámbito del desempeño laboral en el Ayuntamiento de Madrid, y no para un uso particular o profesional de otra índole.

Estas cuentas son creadas y suprimidas a solicitud de las Áreas/Coordinaciones/Gerencias a través de procedimiento existente.

La persona responsable de la cuenta genérica será la única que podrá autorizar el uso de la cuenta a otros empleados y empleadas municipales, así como a personal de proveedores del Ayuntamiento de Madrid o sus OOPP que, por necesidades del servicio, requieran acceder a tales cuentas genéricas.

La persona responsable de la cuenta deberá de gestionar la baja como autorizado de quien no requiera acceder a la cuenta genérica para el desempeño de su actividad, así como de establecer, actualizar y custodiar la contraseña de acceso, y de solicitar la baja de la cuenta genérica cuando ya no sea necesaria.

iii. Servicio de correo electrónico para usuarios no municipales

El personal externo de proveedores que presten servicios para el Ayuntamiento de Madrid o sus OOPP podrá ser usuario autorizado a utilizar tantas cuentas genéricas como sean necesarias para el desempeño de las labores encomendadas en el ámbito municipal.

4.2 Listas de distribución públicas

Las listas de distribución públicas permiten el envío de mensajes a grupos de usuarios y usuarias.

Existirá una persona responsable de cada una de las listas existentes, que deberá mantenerla, dando de alta y baja a los integrantes (cuentas de correo) que la compongan.

Su uso estará restringido a las cuentas permitidas por la persona responsable, de tal forma que únicamente esas cuentas puedan enviar mensajes a la lista concernida.

Cualquier persona responsable de una unidad municipal podrá solicitar de IAM, a través del procedimiento existente, la creación de una lista de distribución pública, responsabilizándose de aportar los datos necesarios y del mantenimiento de la misma. Es responsabilidad de dicha unidad el solicitar su baja cuando ya no sea necesaria.

4.3 Otros componentes del servicio

El servicio de correo electrónico se acompaña del acceso a la Libreta de Direcciones de correo y de la funcionalidad agenda/calendario. Las directrices de uso que figuran en este documento también aplican a estos componentes, que serán responsabilidad del responsable de la cuenta de correo.

5 POLÍTICAS DE USO

El correo electrónico es una herramienta ampliamente implantada en el Ayuntamiento de Madrid y que, como tal, requiere de unas políticas de uso para su correcta utilización.

El correo deberá utilizarse de forma eficiente, teniendo en cuenta que para comunicar y compartir información entre un número elevado de destinatarios/as existen otras herramientas más adecuadas como la Intranet “Ayre” y la red “Ayre social”.

Además, esta amplia implantación y su facilidad de uso ha provocado que el correo electrónico sea un medio a través del cual las organizaciones pueden ser infectadas con software dañino que comprometan la información, los servicios, las redes y los equipos informáticos municipales.

Esta vía de infección puede materializarse de diferentes formas. Pueden ser campañas con correos a grupos pequeños de personas acompañados de ficheros adjuntos ofimáticos dañinos, ficheros ejecutables, enlaces a webs maliciosas, etc. Está demostrado que la utilización de hardware y software de seguridad (cortafuegos, filtros de contenidos, antivirus, etc.) no son contramedidas por sí solas suficientes, por lo que es necesario que las personas usuarias del correo electrónico se atengan a unas recomendaciones básicas en su uso.

A continuación se enumeran diferentes condiciones sobre el uso del correo electrónico, tanto destinadas a su buen uso en general como a su uso seguro en particular.

5.1 Directrices de uso del correo electrónico

- El correo electrónico corporativo debe utilizarse exclusivamente para propósitos profesionales.
- En los mensajes de correo electrónico se debe usar un lenguaje apropiado al entorno profesional para el que está destinado.
- Con carácter general, sólo se proporcionará la dirección de correo electrónico, sea la personal o la genérica, a personas de confianza y del entorno profesional. Se debe evitar introducir esta dirección de correo en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios en el desempeño profesional y con proveedores de confianza, ya que muchos ataques de spam se sirven de direcciones proporcionadas a foros, páginas con carácter comercial y listas de correo.
- Cuando se envíe un mensaje de correo a un conjunto de destinatarios y destinatarias, y entre los cuales se encuentren personas ajenas al Ayuntamiento

de Madrid y Organismos Públicos, se debe utilizar el campo CCO ("copia ciega" o "copia oculta") en lugar de PARA y/o CC.

- No se deben enviar correos de forma masiva. Si se envía por necesidad un correo a un conjunto de destinos, en caso de que sea una necesidad habitual, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO), evitando su visibilidad a todos los receptores del mensaje.
- No se enviarán mensajes que respondan a una 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 al teléfono de incidencias de SICAM (33033).
- Si el ordenador muestra una alerta de correo electrónico con fichero adjunto malicioso, se deberá de notificar el incidente de seguridad a SICAM (33033) y seguir sus instrucciones.
- Antes de enviar un mensaje debería comprobarse la barra de direcciones. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información.
- No debe 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.
- Por regla general, no debe de abrir archivos adjuntos de mensajes cuyo remitente no sea conocido.
- Es conveniente leer atentamente la dirección del remitente por si el correo electrónico es parte de una campaña de malware que utiliza la suplantación del remitente mediante nombres de domino similares utilizando técnicas de omisión (p.e. juan.garcia@gasnatura.com) o de inserción (p.e. juan.garcia@gas-natural.es)
- No debe abrir mensajes de correo sospechosos, con elementos fuera de lo común en el contexto que se trate (remitente, asunto, destinatarios, contenido del mensaje) o que claramente sean "spam".
- En caso de que el correo electrónico tenga un fichero adjunto, hay que verificar la congruencia entre la extensión del fichero y si éste tiene asociado por el sistema operativo un icono reconocible. Por ejemplo, los ficheros asociados al icono de Excel tendrían que tener extensión .xls, .xlsx. En caso contrario, el fichero puede ser dañino.
- Hay que tener especial cuidado con los archivos de Office, tanto de Word como Excel, ya que pueden contener macros con código malicioso. Las posibilidades y acciones que pueden realizarse mediante macros van más allá que la simple interacción con los documentos ofimáticos a la que están destinadas, ya que es posible incluir en ellas un software dañino o programar instrucciones para que el sistema operativo descargue y ejecute un software que permita el control remoto del equipo. Si recibe un archivo adjunto sospechoso, que le solicite habilitar las macros de un documento Office, deberá analizarlo previamente con la herramienta antivirus de que disponga el ordenador. Si accidentalmente abre un documento Word o Excel que pide al titular de la cuenta "habilitar las macros" y

tiene dudas respecto de su legitimidad, se debe cerrar inmediatamente el documento y avisar a SICAM (33033) para que analicen el mensaje sospechoso.

- No abrir ficheros ejecutables en caso de recibirlos mediante correo electrónico. Son ficheros ejecutables aquellos cuya extensión es .exe, .bat, .com, .cpl, .paf, .cmd, .cpl, .js, .jse, .msi, .msp, .mst, .vbs, .vbe, .psc1
- En caso de que el correo electrónico tenga un fichero adjunto, hay que verificar el nombre del fichero para comprobar que no tiene en ninguna parte una combinación de letras que pueda ser interpretada mediante caracteres de lectura inversa como un ejecutable.
- Asimismo, hay que comprobar que el adjunto no tiene un número desproporcionado de espacios en blanco que puedan ocultar su verdadera extensión. Así, un fichero "documento.pdf .exe" podría visualizarse como "documento.pdf..." si el número de espacios en blanco fuera suficientemente elevado.
- Por regla general, no debe de pulsar en los enlaces o links que aparecen dentro de un mensaje, a menos que se trate de un mensaje esperado. Los enlaces incorporados en algunos mensajes pueden dirigir a la persona usuaria del servicio a una web maliciosa o a una página de phising (engaño) haciéndose pasar por sitios web de una institución, banco u organismo. A pesar de que no haya dado la dirección en ninguna lista de distribución, foro, etc. puede recibir mensajes de engaño que son cada vez son más sofisticados. Por ejemplo, la recepción de una factura de precio desorbitado y un enlace para verla, o un paquete que debe retirar y si no pincha en el enlace se le cobrará un dinero, o que ha recibido un premio y debe seguir las instrucciones, o un banco que si no aporta las credenciales se le dará de baja, etc
- Asimismo, también deben de extremarse las precauciones si un correo electrónico recibido solicita descargar y ejecutar un fichero.
- Se debe desactivar la vista previa en la barra de herramientas, ya que utilizar ésta para los mensajes de la bandeja de entrada comporta los mismos riesgos que abrirlos.
- Debe limitar el uso de formato HTML en el mensaje. 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.
- Se desaconseja utilizar el correo electrónico como espacio de almacenamiento. No es la herramienta más adecuada para ello, y la capacidad de espacio en los servidores de correo es limitada. Cuando una cuenta se satura queda mermado su funcionamiento. Es necesario, por tanto, que la persona responsable de la cuenta de correo realice periódicamente tareas de mantenimiento del buzón para evitar el colapso por superar el límite establecido. Para ello se debe:
    - Crear "carpetas archivadas" (extensión pst), bien en la unidad de red asignada o en disco duro local del ordenador de sobremesa, y mover a las mismas los mensajes y documentos adjuntos almacenados en la "bandeja de entrada" o en la "bandeja de elementos enviados" que deseemos conservar.

- Eliminar los mensajes que considere innecesarios y vaciarlos del contenedor de “elementos eliminados”.

5.2 Correos cuyo contenido incluya datos de carácter personal

En el caso de utilizar el correo electrónico para remitir información con datos de carácter personal referentes a ideología, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, creencias, origen étnico o racial, salud, tratamientos de datos genéticos o biométricos, vida y orientación sexual, así como los datos recabados para fines policiales sin consentimiento previo de las personas afectadas y aquellos derivados de actos de violencia de género; la información deberá ir cifrada o bien se deberá utilizar cualquier otro mecanismo que garantice el que la información no sea inteligible ni manipulable por terceros. En el caso de no poder cifrar o evitar la manipulación del correo, quedará prohibido utilizar este medio para el envío de este tipo de datos personales.

6 ACCESO A LAS CUENTAS DE CORREO

Sin perjuicio de la legislación sobre protección de datos de carácter personal, el Ayuntamiento podrá acceder a la información de cuentas de correo almacenada en salvados o a la información de las cuentas de correo vigentes del personal con cuenta de correo municipal, actual y pasado, cuando legítimamente necesite obtener información obrante en las mismas, que permita garantizar el correcto desenvolvimiento de la actividad administrativa, su eficiencia y eficacia, y siempre que no exista otro medio más adecuado de conseguirla. Dicho acceso, salvo situaciones de imposibilidad material (tales como ausencia prolongada, larga enfermedad o baja definitiva) será comunicado previamente a la persona titular o responsable de la cuenta, quien deberá colaborar en lo posible con los administradores de sistemas, aportando información disponible y conocimientos.

El Ayuntamiento también podrá acceder a esta información y a la cuenta de correo, con las debidas garantías y sin comunicación previa a la persona titular o responsable, en los supuestos excepcionales en los que se sospeche pueda concurrir una causa legítima que lo justifique (incumplimiento de los deberes legales de un empleado, en especial el de servir con objetividad a los intereses generales, quebrantamiento o abuso de la confianza por parte del empleado, mala fe o cualquier situación de uso indebido). Este acceso se realizará a petición concreta, específica y motivada en el curso de la tramitación de una información reservada o expediente disciplinario, y la información facilitada por IAM a la unidad peticionaria será proporcionada, idónea, necesaria y razonable a tenor de la solicitud concreta. En caso de existir estas sospechas o indicios de un posible uso indebido, los accesos serán autorizados por la persona responsable de recursos humanos

de quien dependa la persona sujeta a investigación y a petición de la persona que instruya el procedimiento.

6.1 Trazabilidad del servicio de correo.

Para facilitar la trazabilidad del servicio, se generarán registros de cada envío y recepción de correos electrónicos, que contendrán la siguiente información:

- Direcciones de cuentas de correo emisor y destino.
- Fecha y hora de envío.
- Asunto del mensaje.
- Otra información que esté disponible en los registros de actividad

En ningún caso se podrá almacenar el contenido de los correos.

Estos registros deberán disponer de mecanismos que garanticen su seguridad, y el acceso a los mismos deberá estar limitado, exclusivamente, al personal autorizado para ello.

El período de almacenamiento de esta información es de un año, salvo que reglamentariamente exista obligación de conservar los datos durante un periodo diferente.

Por otro lado, también podrán registrarse las siguientes actividades:

- Los accesos e intentos de acceso al servicio.
- Las operaciones relacionadas con la gestión de usuarios.
- Las operaciones relacionadas con la gestión de credenciales de acceso.

6.2 Actuaciones correctivas

Si los administradores del sistema detectan la existencia de un mal uso de los recursos y éste procede de un equipo determinado, pueden tomar las medidas técnicas necesarias para proteger los equipos de la red corporativa, pudiendo desconectar el equipo de la red municipal, ponerlo en cuarentena, etc.

Si un puesto de trabajo conectado a la red interna fuese infectado con un malware que entre sus características incluyera como medio de propagación el correo electrónico, los servicios técnicos de IAM procederán a bloquear el acceso al servicio de correo corporativo desde dicho puesto de trabajo, para garantizar la seguridad de la red, avisando de dicha contingencia.

7 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La dirección de correo electrónico, y otros datos de carácter personal necesarios para la prestación del servicio, serán recogidos y tratados por el Ayuntamiento de Madrid en el tratamiento "Gestión de Identidades" con la finalidad de garantizar la correcta identificación de los usuarios y prestar un servicio correcto y seguro.

El órgano responsable del tratamiento es la Gerencia del Organismo Autónomo Informática del Ayuntamiento de Madrid, calle Albarracín 33, 28037 Madrid ante el que la persona interesada podrá ejercer sus derechos.

El tratamiento está legitimado por Real Decreto 3/2010, modificado por el Real Decreto 951/2015, por el que se aprueba Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS) y que obliga al registro de actividad y garantizar la seguridad de los medios

Los datos personales tratados son de carácter identificativo, y no serán cedidos a terceros salvo en los supuestos legalmente previstos.

8 RESTRICCIONES EN LA RECEPCIÓN DE CORREOS

Los empleados públicos del Ayuntamiento de Madrid podrán solicitar motivadamente al órgano directivo del que dependan inmediatamente la restricción de la recepción y el envío de correos electrónicos por parte de determinadas direcciones de correo electrónico (corporativo o no).

La petición de autorrestricción será autorizada cuando no interfiera con el normal desarrollo de las funciones que tiene encomendadas el peticionario y se llevará a cabo por los servicios y unidades que tengan asignadas las correspondientes funciones operativas en el Organismo Autónomo Informática del Ayuntamiento de Madrid previa solicitud según el procedimiento existente.

Con carácter general, no se autorizarán peticiones de autorrestricción entre personas pertenecientes a una misma Subdirección General, o unidad orgánica equivalente.

En todo caso, se autorizarán las peticiones de autorrestricción que se fundamenten en la tutela de los derechos recogidos en el artículo 14.h) del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

La persona solicitante de la autorrestricción podrá solicitar, en cualquier momento, la ampliación de las cuentas de correo afectadas por la medida de limitación, o el levantamiento de la misma, en la forma prevista en los párrafos anteriores.

9 LEGISLACIÓN APLICABLE

- Ley 1/1982, de 5 de mayo de Protección civil de derechos al honor, intimidad personal y propia imagen.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto Legislativo de 24 de octubre de 1995, por el que se aprueba el Estatuto de los Trabajadores.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y Real Decreto 951/2015, de 23 de octubre, por el que se modifica.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Directivas 95/46, 2002/14 relativas a comunicaciones electrónicas.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
- Instrucción 2/2013, de la Delegada de Gobierno de Economía, Hacienda y Administración Pública, relativa a la implantación del correo electrónico como medio de comunicación interna y con los ciudadanos.
- El Acuerdo de 24 de julio de 2018 del Pleno del Ayuntamiento de Madrid por el que se aprueba la modificación del Reglamento de Ordenación del Personal del Ayuntamiento de Madrid
- Decreto de 21 de octubre de 2013 de la Delegada del Área de Gobierno de Economía, Hacienda y Administración Pública por el que se aprueba la Instrucción 9/2013 en materia de personal para la correcta gestión de los contratos de servicios a fin de evitar incurrir en supuestos de cesión ilegal de trabajadores.