DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

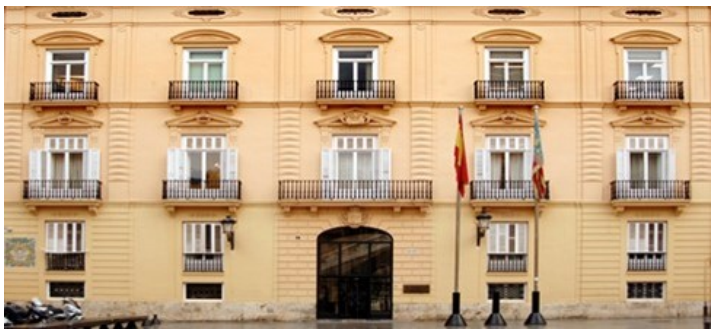
Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 16| Octubre 2021

BUENAS PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO CORPORATIVO

Í N D I C E



BUENAS PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO CORPORATIVO

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

El correo electrónico (e-mail) corporativo es una herramienta de mensajería electrónica puesta a disposición de las personas usuarias de la Diputación de Valencia que lo precisen en el desempeño de su función o actividad, para el envío y recepción de envíos electrónicos. Se trata de una herramienta que aporta grandes beneficios, en cuanto a disponibilidad, accesibilidad, rapidez, posibilidad de envíos a varios destinatarios de varios documentos, etc., y que permite agilizar gran parte de nuestro día a día. 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 parece seguir siendo la herramienta preferida de las personas usuarias de los sistemas de información.

No obstante, dado que a través de estas plataformas fluye una gran parte de la información de la organización,– en particular, datos de carácter personal,– son una de las vías más comunes para la materialización de incidentes de seguridad, ya sea de manera accidental (por ejemplo, remitir documentos confidenciales a quien no se debe, o desvelar direcciones de correo electrónico) o a través de ciberataques (por ejemplo, *spam*, correos de *phishing* que intentan robar credenciales o correos que suplantan entidades o personas).

Mitigar los riesgos del uso del correo electrónico de una forma significativa no siempre requiere de la implantación de complejas medidas técnicas, sino que la concienciación de las personas usuarias de la organización, el sentido común y las buenas prácticas en su uso son las mejores defensas para prevenir y detectar este tipo de incidentes. Por eso, en el presente boletín incidiremos en una serie de cuestiones a tener en cuenta para realizar un uso correcto de nuestras cuentas corporativas de correo electrónico y así proteger de manera adecuada nuestra organización.

DADO QUE A TRAVÉS DEL CORREO ELECTRÓNICO FLUYE UNA GRAN PARTE DE LA INFORMACIÓN DE LA ORGANIZACIÓN,- EN PARTICULAR, DATOS DE CARÁCTER PERSONAL,- ES UNA DE LAS VÍAS MÁS COMUNES PARA LA MATERIALIZACIÓN DE INCIDENTES DE SEGURIDAD. MITIGAR LOS RIESGOS DEL USO DEL CORREO ELECTRÓNICO DE UNA FORMA SIGNIFICATIVA REQUIERE DE BUENAS PRÁCTICAS EN SU USO.

BUENAS PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO CORPORATIVO

Uso exclusivo para la realización de funciones encomendadas. – El correo corporativo debe utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal.

Contraseña segura. – Utiliza una contraseña segura para acceder al correo electrónico. La contraseña no deber contener el nombre de la cuenta de la persona usuaria o partes del nombre completo de la persona usuaria en más de dos caracteres consecutivos. Debe tener una longitud mínima de ocho (8) caracteres e incluir caracteres de tres de las siguientes categorías: mayúsculas, minúsculas, números y caracteres no alfanuméricos (por ejemplo, !, $, #, %). Trata de renovar la contraseña periódicamente.

Revelación de contraseñas. – No reveles o entregues, bajo ningún concepto, tus credenciales de acceso al correo electrónico a otra persona, ni las mantengas por escrito a la vista o al alcance de terceros.

Correo web. – Evita marcar la opción de recordar contraseña en los accesos al correo a través de la web (*webmail*). Éstas podrían ser recuperadas en caso de infección por determinados tipos de *malware*.

Identificación del remitente. – Identifica los remitentes antes de abrir un correo electrónico. Si sospechas que ha sido suplantado, contacta con el remitente por otro medio para confirmarlo.

Análisis de adjuntos. – Analiza cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. Si sospechas de su autenticidad, no lo descargues ni lo abras, y notifica esta circunstancia al departamento de Protección de Datos y Seguridad de la Información.

Inspección de enlaces. – Examina atentamente los enlaces incluidos en los correos antes de acceder a ellos. Fíjate en elementos sospechosos, como caracteres de más o de menos u homógrafos (por ejemplo, 0 en lugar de O).

Spam (correo basura). – Nunca respondas al correo basura. Si respondes, confirmarás que la cuenta está activa, por lo que podrías ser blanco de futuros ataques. Agrégalo a la lista de spam y elimínalo.

Copia oculta (CCO). – Utiliza la copia oculta cuando envíes correos a múltiples direcciones y estos no tengan por qué conocer la dirección de correo electrónico del resto de personas destinatarias.

Reenvío de correos. – Asegúrate de que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

Redes públicas. – Evita consultar el correo corporativo si estás conectado a redes públicas.

Remisión de datos sensibles. – Cifra los mensajes de correo que contengan información de carácter sensible.

Notificación de anomalías. – Notifica a este Departamento cualquier tipo de anomalía detectada en el uso del correo electrónico

REALIZANDO UN USO CORRECTO DE NUESTRAS CUENTAS CORPORATIVAS DE E-MAIL PROTEGEREMOS NUESTRA ORGANIZACIÓN.

¿PUEDEN SANCIONAR A LA DIPUTACIÓN DE VALENCIA POR UN USO INDEBIDO POR PARTE DE LOS USUARIOS DEL E-MAIL CORPORATIVO?

Sin perjuicio de la consecuente depuración interna de responsabilidades ante la Agencia Española de Protección de Datos es la Diputación de Valencia quien respondería por toda incidencia resultante del mal uso por parte de los usuarios de sus cuentas corporativas de correo electrónico. Así mismo, la Corporación quedaría plenamente comprometida por el daño reputacional que causa la exposición pública del incidente y/o la noticia de una sanción (apercibimiento) por parte de la AEPD.

A continuación, hacemos repaso de algunos casos ilustrativos que llegaron a ocupar por las autoridades de control en materia de protección de datos, en concreto por un inadecuado uso del correo electrónico:

En el **Procedimiento Sancionador Nº: PS/00095/2020**, la Agencia Española de Protección de Datos (AEPD) sancionó a un Ayuntamiento por **remitir una reclamación, por correo electrónico, revelando al reclamado la dirección de correo electrónico y el DNI del reclamante.** Manifiesta la AEPD que remitir la dirección de correo electrónico y el DNI del reclamante sin utilizar la opción de Copia Oculta (CCO) para efectuar el envío, supone la vulneración de los principios de «limitación de la finalidad» e «integridad y confidencialidad».

En el **Procedimiento Sancionador Nº: PS/00376/2020**, la AEPD sancionó a una asesoría por **adjuntar a un correo electrónico dirigido a un cliente, por error, copia de un certificado de reclamación de deuda perteneciente a un tercero**, vulnerando el deber de confidencialidad.

En el **Procedimiento Sancionador Nº: 19/2020**, la APDCAT sancionó a un Ayuntamiento por **enviar un correo electrónico sin copia oculta a todos los participantes no ganadores de un sorteo de entradas**, por lo que todas las personas pudieron acceder a la dirección de correo del resto de participantes no seleccionados, vulnerando el principio de confidencialidad.

En el **Procedimiento Sancionador Nº: 21/2017**, la APDCAT sancionó a un centro educativo público por la **transmisión de datos especialmente protegidos a través de correo electrónico sin cifrar.**

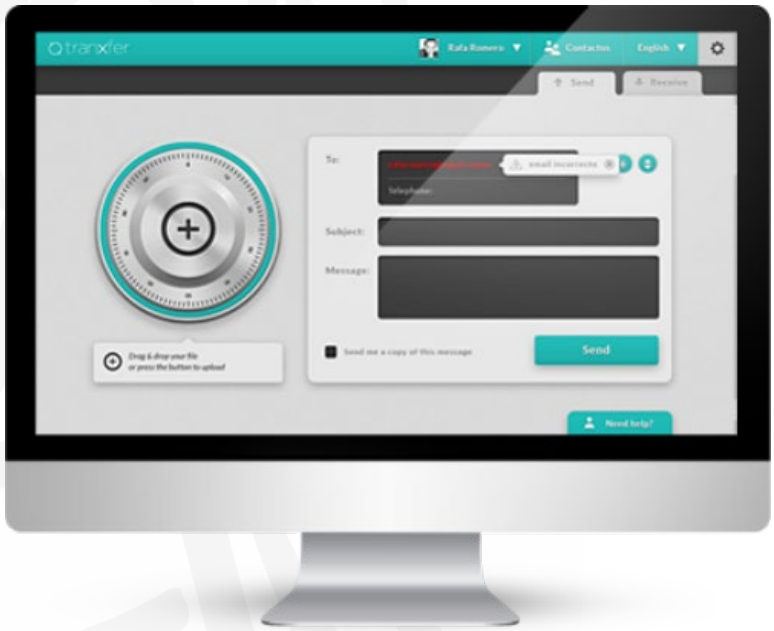
EL USO INADECUADO DEL CORREO ELECTRÓNICO POR PARTE DE LAS PERSONAS USUARIAS DE LA DIPUTACIÓN DE VALÈNCIA PODRÍA CONLLEVAR UNA SANCIÓN DE APERCIBIMIENTO PARA LA CORPORACIÓN, ACOMPAÑADA DE LAS MEDIDAS QUE CONSIDERE LA AEPD. ASIMISMO, HA DE TENERSE EN CUENTA EL DAÑO REPUTACIONAL QUE LA SANCIÓN, ASÍ COMO LA DIVULGACIÓN SOBRE EL INCIDENTE, CAUSARÍAN A LA CORPORACIÓN.

HERRAMIENTAS COMPATIBLES CON EL USO DEL E-MAIL CORPORATIVO PARA MAYORES GARANTÍAS CONFIDENCIALIDAD

Uno de los usos que damos al correo electrónico corporativo es la comunicación interna y, dentro de este constante proceso, el intercambio de archivos. Siendo también de aplicación para el envío de ficheros fuera de la Corporación, existen herramientas, soluciones tecnológicas desarrolladas a tal efecto, que ofrecen una mayor confianza para con estos procesos.

La Diputación de València apostó en su día por "Tranxfer", aplicativo con el que se cuenta para la transferencia segura de archivos y que está accesible desde la intranet.

A diferencia de otros sistemas de uso doméstico o particular, Tranxfer es una herramienta que permite la compartición de archivos tanto de la propia Corporación como con destinatarios externos (proveedores, interesados, otras Administraciones, etcétera), controlando y eliminando el riesgo de fuga de información entre las mismas. Tranxfer, proyecto desarrollado por el holding empresarial IRIS para la creación de productos innovadores para entidades (B2B), controla el ciclo de vida del intercambio de archivos, reduciendo al mínimo los 'agujeros' de seguridad propios de entornos con políticas de confidencialidad.



El funcionamiento de Tranxfer es relativamente sencillo: para realizar el envío, el usuario que necesita transferir documentación a una persona puede facilitar el número de móvil del receptor, que recibe un mail con el enlace para la descarga y un código de autorización en el móvil.

Así, Tranxfer permite disponer en todo momento de la información referente a dónde se encuentran los datos y ejecución de los pasos dentro de este mismo proceso: emisor, destinatario, nombre del fichero, tamaño, fecha, hora de envío, hora de descarga, etc. El objetivo de la utilización de Tranxfer es reducir el uso del mail como sistema de envío no seguro y reducir costes, centralizando y controlando todos los archivos que salen y entran por parte de las empresas.

EXISTEN HERRAMIENTAS, SOLUCIONES TECNOLÓGICAS DESARROLLADAS A TAL EFECTO, COMO TRANXFER (A DISPOSICIÓN DESDE LA INTRANET) QUE OFRECEN UNA MAYOR CONFIANZA PARA CON LOS PROCESOS DE INTERCAMBIO DE ARCHIVOS, TANTO INTERNAMENTE, COMO FUERA DE LA CORPORACIÓN.

MATERIAL COMPLEMENTARIO

- ¿Seguridad en el correo electrónico? Sí, en tan solo 10 pasos (INCIBE). Consulta este enlace.
- Correo electrónico. Informe de buenas prácticas (CCN). Consulta este enlace.
- Privacidad y Seguridad en Internet. Ficha 14: Quiero proteger mi correo electrónico (AEPD, INCIBE, OSI). Consulta este enlace.
- Uso del correo electrónico (INCIBE). Consulta este enlace.
- Procedimiento Sancionador Nº: PS/00095/2020 (AEPD). Consulta este enlace.
- Procedimiento Sancionador Nº: PS/00376/2020 (AEPD). Consulta este enlace.
- Procedimiento Sancionador Nº: 19/2020 (APDCAT). Consulta este enlace.
- Procedimiento Sancionador Nº: 21/2017 (APDCAT). Consulta este enlace.
- Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, aprobado por acuerdo del Pleno de la Corporación de fecha 18 de junio de 2013 -BOP 159, de 6 de julio-.
- Decreto nº 6111, de 26 de junio de 2015, Normas de Seguridad para los Usuarios de los Sistemas de Información. Diputación Provincial de Valencia.

NOTICIAS

- **La Administración Pública Canaria se moderniza: elimina el fax y usará el correo electrónico.** La implantación supondrá un ahorro económico para las arcas autonómicas. Sigue leyendo en este enlace.
- **La Agencia Tributaria advierte de una serie de estafas por correo electrónico y SMS: no abras estos mensajes.** Los ciberdelincuentes mandan mensajes a las víctimas suplantando la identidad de la Administración para conseguir sus datos secretos. Sigue leyendo en este enlace.
- **El 97% de los emails que usan los funcionarios está desprotegido frente a robos de identidad.** Los servicios públicos españoles han recibido en los últimos meses una severa oleada de ciberataques. Sigue leyendo en este enlace.
- **Denuncian al Ayuntamiento por infringir la legislación de protección de datos personales.** El Centro Municipal de Información a la Mujer, respondiendo a unas inscripciones que se realizaban por correo electrónico, no sólo se envió respuesta con todas las direcciones de las solicitantes visibles, adjuntando un formulario para cumplimentar con los datos personales, sino que posteriormente la denunciante continuó recibiendo correos electrónicos dirigidos al CMIM con los datos personales de las otras solicitantes, entre los que figuraban nombre y apellidos, DNI, fecha de nacimiento, dirección de correo electrónico y teléfono, lugar de empadronamiento o, incluso, patologías o enfermedades previas. Sigue leyendo en este enlace.