DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí núm. 16| Octubre 2021

BONES PRÀCTIQUES EN L'ÚS DEL CORREU ELECTRÒNIC CORPORATIU

DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

ÍNDEX

BONES PRÀCTIQUES EN L'ÚS DEL CORREU ELECTRÒNIC CORPORATIU

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades s Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

El correu electrònic (e-mail) corporatiu és una eina de missatgeria electrònica posada a la disposició de les persones usuàries de la Diputació de València que ho precisen en l'acompliment de la seua funció o activitat, per a l'enviament i recepció d'enviaments electrònics.

Es tracta d'una eina que aporta grans beneficis, quant a disponibilitat, accessibilitat, rapidesa, possibilitat d'enviaments a diversos destinataris de diversos documents, etc., i que permet agilitar gran part del nostre dia a dia. A pesar que en els últims anys han sorgit multitud de tecnologies i eines col·laboratives per a facilitar la comunicació i l'intercanvi de fitxers, el correu electrònic sembla continuar sent l'eina preferida de les persones usuàries dels sistemes d'informació.

No obstant això, atés que a través d'aquestes plataformes flueix una gran part de la informació de l'organització,– en particular, dades de caràcter personal,– són una de les vies més comunes per a la materialització d'incidents de seguretat, ja siga de manera accidental (per exemple, remetre documents confidencials a qui no es deu, o revelar adreces de correu electrònic) o a través de ciberatacs (per exemple, *spam*, correus de *phishing* que intenten robar credencials o correus que suplanten entitats o persones).

Mitigar els riscos de l'ús del correu electrònic d'una forma significativa no sempre requereix de la implantació de complexes mesures tècniques, sinó que la conscienciació de les persones usuàries de l'organització, el sentit comú i les bones pràctiques en el seu ús són les millors defenses per a previndre i detectar aquest tipus d'incidents. Per això, en el present butlletí incidirem en una sèrie de qüestions a tindre en compte per a realitzar un ús correcte dels nostres comptes corporatius de correu electrònic i així protegir de manera adequada la nostra organització.

ATÉS QUE A TRAVÉS DEL CORREU ELECTRÒNIC FLUEIX UNA GRAN PART DE LA INFORMACIÓ DE L'ORGANITZACIÓ,- EN PARTICULAR, DADES DE CARÀCTER PERSONAL,- ÉS UNA DE LES VIES MÉS COMUNES PER A LA MATERIALITZACIÓ D'INCIDENTS DE SEGURETAT. MITIGAR ELS RISCOS DE L'ÚS DEL CORREU ELECTRÒNIC D'UNA FORMA SIGNIFICATIVA REQUEREIX DE BONES PRÀCTIQUES EN EL SEU ÚS.

BONES PRÀCTIQUES EN L'ÚS DEL CORREU ELECTRÒNIC CORPORATIU

Ús exclusiu per a la realització de funcions encomanades. – El correu corporatiu ha d'utilitzar-se, exclusivament, per a la realització de les funcions encomanades al personal.

Contrasenya segura. – Utilitza una contrasenya segura per a accedir al correu electrònic. La contrasenya no haver de contindre el nom del compte de la persona usuària o parts del nom complet de la persona usuària en més de dos caràcters consecutius. Ha de tindre una longitud mínima de huit (8) caràcters i incloure caràcters de tres de les següents categories: majúscules, minúscules, números i caràcters no alfanumèrics (per exemple, !, $, #, %). Tracta de renovar la contrasenya periòdicament.

Revelació de contrasenyes. – No reveles o entregues, en cap concepte, les teues credencials d'accés al correu electrònic a una altra persona, ni les mantingues per escrit a la vista o a l'abast de tercers.

Correu web. – Evita marcar l'opció de recordar contrasenya en els accessos al correu a través de la web (*webmail*). Aquestes podrien ser recuperades en cas d'infecció per determinats tipus de malware .

Identificació del remitent. – Identifica els remitents abans d'obrir un correu electrònic. Si sospites que ha sigut suplantat, contacta amb el remitent per un altre mitjà per a confirmar-lo.

Anàlisi d'adjunts. – Analitza acuradament els adjunts de correus de remitents desconeguts abans d'obrir-los. No han d'obrir-se ni executar-se fitxers de fonts no fiables, ja que podrien contindre virus o codi maliciós. Si sospites de la seua autenticitat, no ho descarregues ni ho òbrigues, i notifica aquesta circumstància al departament de Protecció de Dades i Seguretat de la Informació.

Inspecció d'enllaços. – Examina atentament els enllaços inclosos en els correus abans d'accedir a ells. Fixa't en elements sospitosos, com a caràcters de més o de menys o homògrafs (per exemple, 0 en lloc d'O).

Spam (correu fem). – Mai respongues al correu fem. Si respons, confirmaràs que el compte està actiu, per la qual cosa podries ser blanc de futurs atacs. Agrega-ho a la llista de spam i elimina-ho.

Còpia oculta (CCO). – Utilitza la còpia oculta quan envies correus a múltiples adreces i aquests no tinguen per què conéixer l'adreça de correu electrònic de la resta de persones destinatàries.

Reexpedició de correus. – Assegura't que les reexpedicions de missatges prèviament rebuts es transmeten únicament als destinataris apropiats.

Xarxes públiques. – Evita consultar el correu corporatiu si estàs connectat a xarxes públiques.

Remissió de dades sensibles. – Xifra els missatges de correu que continguen informació de caràcter sensible.

Notificació d'anomalies. – Notifica a aquest Departament qualsevol tipus d'anomalia detectada en l'ús del correu electrònic

REALITZANT UN ÚS CORRECTE DELS NOSTRES COMPTES CORPORATIUS D'E-MAIL PROTEGIREM LA NOSTRA ORGANITZACIÓ.

PODEN SANCIONAR A LA DIPUTACIÓ DE VALÈNCIA PER UN ÚS INDEGUT PER PART DELS USUARIS DE L'E-MAIL CORPORATIU?

Sense perjudici de la conseqüent depuració interna de responsabilitats davant l'Agència Espanyola de Protecció de Dades és la Diputació de València qui respondria per tota incidència resultant del mal ús per part dels usuaris dels seus comptes corporatius de correu electrònic. Així mateix, la Corporació quedaria plenament compromesa pel mal reputacional que causa l'exposició pública de l'incident i/o la notícia d'una sanció (prevenció) per part de l'AEPD.

A continuació, fem repàs d'alguns casos il·lustratius que van arribar a ocupar per les autoritats de control en matèria de protecció de dades, en concret per un inadequat ús del correu electrònic:

En el **Procediment Sancionador Núm.: PS/00095/2020**, l'Agència Espanyola de Protecció de Dades (AEPD) va sancionar a un Ajuntament per remetre **una reclamació, per correu electrònic, revelant al reclamat l'adreça de correu electrònic i el DNI del reclamant.** Manifesta l'AEPD que remetre l'adreça de correu electrònic i el DNI del reclamant sense utilitzar l'opció de Còpia Oculta (CCO) per a efectuar l'enviament, suposa la vulneració dels principis de «limitació de la finalitat» i «integritat i confidencialitat».

En el **Procediment Sancionador Núm.: PS/00376/2020**, l'AEPD va sancionar a una assessoria per adjuntar **a un correu electrònic dirigit a un client, per error, còpia d'un certificat de reclamació de deute pertanyent a un tercer**, vulnerant el deure de confidencialitat.

En el **Procediment Sancionador Núm.: 19/2020**, la APDCAT va sancionar a un Ajuntament per enviar **un correu electrònic sense còpia oculta a tots els participants no guanyadors d'un sorteig d'entrades**, per la qual cosa totes les persones van poder accedir a l'adreça de correu de la resta de participants no seleccionats, vulnerant el principi de confidencialitat.

En el **Procediment Sancionador Núm.: 21/2017**, la APDCAT va sancionar a un centre educatiu públic per la **transmissió de dades especialment protegides a través de correu electrònic sense xifrar.**

L'ÚS INADEQUAT DEL CORREU ELECTRÒNIC PER PART DE LES PERSONES USUÀRIES DE LA DIPUTACIÓ DE VALÈNCIA PODRIA COMPORTAR UNA SANCIÓ DE PREVENCIÓ PER A LA CORPORACIÓ, ACOMPANYADA DE LES MESURES QUE CONSIDERE L'AEPD. AIXÍ MATEIX, HA DE TINDRE'S EN COMPTE EL MAL REPUTACIONAL QUE LA SANCIÓ, AIXÍ COM LA DIVULGACIÓ SOBRE L'INCIDENT, CAUSARIEN A LA CORPORACIÓ.

EINES COMPATIBLES AMB L'ÚS DE L'E-MAIL CORPORATIU PER A MAJORS GARANTIES CONFIDENCIALITAT

Un dels usos que donem al correu electrònic corporatiu és la comunicació interna i, dins d'aquest constant procés, l'intercanvi d'arxius. Sent també d'aplicació per a l'enviament de fitxers fora de la Corporació, existeixen eines, solucions tecnològiques desenvolupades a aquest efecte, que ofereixen una major confiança envers aquests processos.

La Diputació de València va apostar en el seu moment per "Tranxfer", aplicatiu amb el qual es compta per a la transferència segura d'arxius i que està accessible des de la intranet.

A diferència d'altres sistemes d'ús domèstic o particular, Tranxfer és una eina que permet la compartició d'arxius tant de la pròpia Corporació com amb destinataris externs (proveïdors, interessats, altres Administracions, etcètera), controlant i eliminant el risc de fugida d'informació entre aquestes. Tranxfer, projecte desenvolupat pel hòlding empresarial IRIS per a la creació de productes innovadors per a entitats (B2B), controla el cicle de vida de l'intercanvi d'arxius, reduint al mínim els 'forats' de seguretat propis d'entorns amb polítiques de confidencialitat.

El funcionament de Tranxfer és relativament senzill: per a realitzar l'enviament, l'usuari que necessita transferir documentació a una persona pot facilitar el número de mòbil del receptor, que rep un mail amb l'enllaç per a la descàrrega i un codi d'autorització en el mòbil.

Així, Tranxfer permet disposar en tot moment de la informació referent a on es troben les dades i execució dels passos dins d'aquest mateix procés: emissor, destinatari, nom del fitxer, grandària, data, hora d'enviament, hora de descàrrega, etc. L'objectiu de la utilització de Tranxfer és reduir l'ús del mail com a sistema d'enviament no segur i reduir costos, centralitzant i controlant tots els arxius que ixen i entren per part de les empreses.

EXISTEIXEN EINES, SOLUCIONS TECNOLÒGIQUES DESENVOLUPADES A AQUEST EFECTE, COM TRANXFER (A DISPOSICIÓ DES DE LA INTRANET) QUE OFEREIXEN UNA MAJOR CONFIANÇA ENVERS ELS PROCESSOS D'INTERCANVI D'ARXIUS, TANT INTERNAMENT, COM FORA DE LA CORPORACIÓ.

MATERIAL COMPLEMENTARIO

- Seguretat en el correu electrònic? Sí, en tan sols 10 passos (INCIBE). Consulta aquest enllaç.
- Correu electrònic. Informe de bones pràctiques (CCN). Consulta aquest enllaç.
- Privacitat i Seguretat en Internet. Fitxa 14: Vull protegir el meu correu electrònic (AEPD, INCIBE, OSI). Consulta aquest enllaç.
- Ús del correu electrònic (INCIBE). Consulta aquest enllaç.
- Procediment Sancionador Nº: PS/00095/2020 (AEPD). Consulta aquest enllaç.
- Procediment Sancionador Nº: PS/00376/2020 (AEPD). Consulta aquest enllaç.
- Procediment Sancionador Nº: 19/2020 (APDCAT). Consulta aquest enllaç.
- Procediment Sancionador Nº: 21/2017 (APDCAT). Consulta aquest enllaç.
- Reglament de Política de Seguretat i de la Protecció de Dades de Caràcter Personal en la Diputació Provincial de València, aprovat per acord del Ple de la Corporació de data 18 de juny de 2013 -BOP 159, de 6 de juliol.
- Decret núm. 6111, de 26 de juny de 2015, Normes de Seguretat per als Usuaris dels Sistemes d'Informació. Diputació Provincial de València.

NOTÍCIES

- **L'Administració Pública Canària es modernitza: elimina el fax i usarà el correu electrònic.** La implantació suposarà un estalvi econòmic per a les arques autonòmiques. Continua llegint en aquest enllaç.
- **L'Agència Tributària adverteix d'una sèrie d'estafes per correu electrònic i SMS: no òbrigues aquests missatges.** Els ciberdelincuents envien missatges a les víctimes suplantant la identitat de l'Administració per a aconseguir les seues dades secretes. Continua llegint en aquest enllaç.
- **El 97% dels emails que usen els funcionaris està desprotegit enfront de robatoris d'identitat.** Els serveis públics espanyols han rebut en els últims mesos una severa onada de ciberatacs. Continua llegint en aquest enllaç.
- **Denuncien a l'Ajuntament per infringir la legislació de protecció de dades personals.** El Centre Municipal d'Informació a la Dona, responent a unes inscripcions que es realitzaven per correu electrònic, no sols es va enviar resposta amb totes les adreces de les sol·licitants visibles, adjuntant un formulari per a emplenar amb les dades personals, sinó que posteriorment la denunciant va continuar rebent correus electrònics dirigits al CMIM amb les dades personals de les altres sol·licitants, entre els quals figuraven nom i cognoms, DNI, data de naixement, adreça de correu electrònic i telèfon, lloc d'empadronament o, fins i tot, patologies o malalties prèvies. Continua llegint en aquest enllaç.