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 N.º 9| Març 2021

MESURES DE SEGURETAT EN EL LLOC DE TREBALL

ÍNDEX

MESURES DE SEGURETAT EN EL LLOC DE TREBALL

Vos convidem a traslladar-nos les temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Les peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdssi@dival.es

SUSCRIPCIONS

Si desitja subscriure't a la nostra publicació accedisca al següent enllaç

INTRODUCCIÓ

El bon funcionament d'una organització depén, en gran manera, dels seus sistemes d'informació i de la informació que en ells s'emmagatzema. La gestió d'aquesta informació es realitza des del lloc de treball, ja siga des de dispositius tecnològics com no tecnològics.

El concepte de lloc de treball va més enllà de la ubicació física on els usuaris dels sistemes d'informació de l'organització exerceixen les seues funcions diàries. El lloc de treball ha anat estenent-se amb la incorporació dels nous dispositius tecnològics com: ordinadors de sobretaula, portàtils, telèfons mòbils, tauletes, dispositius d'emmagatzematge extraïbles, impressores de xarxa, escàners, etc.

Gran part dels incidents de seguretat se solen generar dins de la pròpia organització i, en moltes ocasions, de manera accidental. Per aquest motiu, un element vital per a evitar incidents relacionats amb la seguretat de la informació és la implantació de mesures de seguretat en el lloc de treball.

Mitigar els riscos del lloc de treball d'una forma significativa no sempre requereix de la implantació de complexes mesures tècniques, sinó que es tracta d'establir una cultura de la seguretat de la informació i posar en marxa mesures tècniques i organitzatives adaptades a les necessitats del lloc de treball que són, en la majoria dels casos, senzilles. L'aplicació d'aquestes mesures, al costat d'un adequat pla de formació i conscienciació de les persones treballadores que gestionen la informació des dels seus llocs de treball, ens ajudarà a protegir de manera adequada la nostra organització.

"MITIGAR ELS RISCOS DEL LLOC DE TREBALL D'UNA FORMA SIGNIFICATIVA NO REQUEREIX DE LA IMPLANTACIÓ DE COMPLEXES MESURES TÈCNIQUES, SINÓ QUE ES TRÀFIC D'ESTABLIR UNA CULTURA DE LA SEGURETAT DE LA INFORMACIÓ I POSAR EN MARXA MESURES TÈCNIQUES I ORGANITZATIVES ADAPTADES A LES NECESSITATS DEL LLOC DE TREBALL QUE SÓN, EN LA MAJORIA DELS CASOS, SENZILLES".

ESCENARIS DE RISC

No sempre els incidents de seguretat es produeixen per usuaris malintencionats. Sovint, es tracta d'usuaris que duen a terme pràctiques no recomanables, que poden ser aprofitades per un atacant extern o intern, o simplement portar associades conseqüències indesitjables.

Vegem, com a exemple, alguns escenaris de risc que ens podem trobar, de manera habitual, en el nostre lloc de treball:

Un usuari deté l'antivirus corporatiu perquè li impedeix dur a terme alguna acció. Més tard, executa un arxiu que li arriba per correu electrònic, infectant el seu equip i tota la xarxa de l'organització.

Un usuari tira a la paperera els exàmens de l'últim procés de selecció, que acaben en un contenidor i són recollits per una tercera persona.

Un usuari còpia en un pendrive documentació per a continuar treballant des de casa. El pendrive es perd en l'autobús, algú el troba i la informació acaba publicant-se.

Un usuari embene el seu portàtil personal. Encara que no es tracta d'una eina professional, era habitual que ho utilitzara per a gestionar i guardar informació corporativa. Mitjançant un senzill programa de recuperació, el comprador recupera la informació i la fa pública.

Un usuari deixa en la safata de la impressora documents que contenen dades personals. Un ciutadà descontent aprofita que no li veu ningú per a agafar els documents.

Un usuari rep un correu electrònic d'un destinatari desconegut que li encoratja a descarregar un arxiu adjunt que conté un codi maliciós, tècnica a través de la qual aconsegueix obtindre informació confidencial de l'organització.

"NO SEMPRE ELS INCIDENTS DE SEGURETAT ES PRODUEIXEN PER USUARIS MALINTENCIONATS. SOVINT, ES TRACTA D'USUARIS QUE DUEN A TERME PRÀCTIQUES NO RECOMANABLES, QUE PODEN SER APROFITADES PER UN ATACANT EXTERN O INTERN, O SIMPLEMENT PORTAR ASSOCIADES CONSEQÜÈNCIES INDESITJABLES".

QUÈ PODEM FER PER A EVITAR-HO?
MESURES DE SEGURETAT

Vistos els escenaris anteriors, és lògic preguntar-se com podem evitar o mitigar els riscos. El primer i fonamental és implantar una **Política de Seguretat** interna de l'organització, que transmeta als usuaris dels sistemes d'informació de l'organització les obligacions i bones pràctiques en relació amb la seguretat de la informació. I és que, la seguretat de la informació és un esforç conjunt, que requereix la implicació i participació de totes les persones usuàries que utilitzen els sistemes d'informació per a l'acompliment del seu treball, i en el seu cas, el personal extern vinculat a prestacions de serveis.

En la Diputació de València, comptem amb el **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-, l'article del qual 37.1 estableix que hauran d'elaborar-se un conjunt de regles i directrius de caràcter obligatori que desenvolupen el contingut d'aquesta Política.

Per Decret núm. 6111, de 26 de juny de 2015, es van aprovar les **Normes de Seguretat per als Usuaris dels Sistemes d'Informació**, d'aplicació a tots els sistemes d'informació TIC, així com a aquells sistemes d'informació de qualsevol naturalesa que tracten dades de caràcter personal, que siguen de la titularitat de la Diputació de València o la gestió o la responsabilitat de la qual tinga encomanada, com és el cas de la informació municipal. Aquestes són algunes de les mesures contemplades:

MITJANS TECNOLÒGICS

- L'ús dels recursos facilitats als usuaris per l'organització per al desenvolupament de l'activitat, amb finalitats diferents als autoritzats, està estrictament prohibit.
- No està permés alterar la configuració maquinari dels equips ni connectar altres dispositius a aquests a iniciativa de l'usuari, així com variar la seua ubicació.
- No està permés alterar la configuració programari dels equips, desinstal·lar o instal·lar programes diferents a la configuració establida pel Servei d'Informàtica.
- No està permesa la instal·lació, utilització o connexió a la xarxa corporativa de qualsevol mitjà tecnològic diferent dels admesos, habilitats i configurats pel Servei d'Informàtica, sense comptar amb la seua autorització.
- No està permés emmagatzemar informació privada, de qualsevol naturalesa, en els recursos d'emmagatzematge compartits.

DISPOSITIUS PORTÀTILS I MÒBILS

- Està prohibit utilitzar dispositius portàtils i mòbils no proporcionats per la Corporació per a emmagatzemar, accedir, transmetre o tractar de qualsevol altra manera informació, excepte si es compta amb autorització.

- En principi, els dispositius portàtils i mòbils hauran d'utilitzar-se únicament per a fins professionals, no per a fins privats.

- Aquest tipus de dispositius estarà sota la custòdia de l'usuari que els utilitze, el qual haurà d'adoptar les mesures necessàries per a evitar danys o sostracció, així com l'accés a ells per part de persones no autoritzades.

- La pèrdua o sostracció d'aquests dispositius s'haurà de posar immediatament en coneixement del Servei d'Informàtica de la Corporació, per a l'adopció de les mesures que corresponguen i a l'efecte de baixa en l'inventari.

- Els usuaris d'aquests dispositius hauran de realitzar connexions periòdiques a la xarxa corporativa, segons les instruccions proporcionades pel Servei d'Informàtica, per a permetre l'actualització d'aplicacions, sistema operatiu, signatures d'antivirus i altres mesures de seguretat.

- Quan es modifiquen les circumstàncies professionals (terme d'una tasca, canvi de lloc o funcions, cessament en el càrrec, etc.) que van originar el lliurament d'un recurs informàtic mòbil, l'usuari el retornarà al Servei d'Informàtica de la Corporació, a fi de conducta a l'esborrat segur de la informació emmagatzemada i, en el seu cas, restaurar l'equip al seu estat original perquè puga ser assignat a un nou usuari.

- Està prohibit utilitzar suports electrònics d'informació no proporcionats per la Corporació per a emmagatzemar informació, excepte si es tracta d'informació classificada com a PÚBLICA i es compta amb l'autorització corresponent.

- Si es produïra la sostracció, pèrdua o accés indegut als suports d'informació haurà de posar-se en coneixement del Responsable de Seguretat dels Sistemes d'Informació, a través del sistema de notificació d'incidències de seguretat

SUPORTS ELECTRÒNICS DE INFORMACIÓ

- En el trasllat de suports d'informació s'adoptaran les pertinents mesures per a evitar la sostracció, pèrdua o accés indegut a la informació durant el seu transport, especialment quan la informació continguda en el suport no haja sigut objecte de xifratge. Es disposarà d'un procediment rutinari que acare les eixides amb les arribades i llevant les alarmes pertinents quan es detecte algun incident. En cas de sostracció, pèrdua o accés indegut a la informació durant el seu transport haurà de posar-se en coneixement del Responsable de Seguretat dels Sistemes d'Informació, a través del sistema de notificació d'incidències de seguretat.

CORREU ELECTRÒNIC

- Únicament podran utilitzar-se les eines i programes de correu electrònic subministrats, instal·lats i configurats pel Servei d'Informàtica de la Diputació de València.

- El correu corporatiu haurà d'utilitzar-se, exclusivament, per a la realització de les funcions encomanades al personal, evitant l'ús privat d'aquest.

INTERNET

- Només es podrà accedir a Internet mitjançant els navegadors subministrats i configurats pel Servei d'Informàtica en els llocs d'usuari. No podrà alterar-se la configuració del mateix ni utilitzar un navegador alternatiu sense la deguda autorització del Servei d'Informàtica.

- La utilització d'Internet ha d'obeir a fins professionals, tenint sempre en compte que s'estan utilitzant recursos informàtics restringits i escassos. L'accés a Internet per a fins personals tindrà caràcter extraordinari, havent-se de limitar la seua utilització dins d'un temps raonable que no interferisca en el rendiment professional ni en l'eficiència dels recursos informàtics corporatius

IMPRESSORES, FOTOCOPIADORES, ESCÀNERS I FAXOS

- Amb caràcter general hauran d'utilitzar-se les impressores en xarxa i les fotocopiadores corporatives. Excepcionalment podran instal·lar-se impressores locals, gestionades per un lloc de treball d'usuari. En aquest cas, la instal·lació anirà precedida de l'autorització pertinent per part del responsable del peticionari.

- Quan s'imprimisca, fotocopie, digitalitze o es remeta per fax documentació, haurà de romandre el menor temps possible en les safates d'eixida dels equips implicats, per a evitar que terceres persones puguen accedir a aquesta.

- Convé no oblidar retirar els originals de la fotocopiadora, impressora, escàner o fax una vegada finalitzat el procés corresponent.

- Si es trobara documentació abandonada en una fotocopiadora, impressora, escàner o fax, l'usuari intentarà localitzar al seu propietari perquè aquest la reculla immediatament. En cas de desconéixer al seu propietari o no localitzar-lo, el posarà immediatament en coneixement del superior jeràrquic.

- Amb caràcter general, quan es digitalitzen documents l'usuari haurà de ser especialment acurat amb la selecció del directori compartit on hauran d'emmagatzemar-se les imatges obtingudes, especialment si contenen informació no classificada com a PÚBLICA.

CONTROL D'ACCESSOS ALS SISTEMES D'INFORMACIÓ

- Els mecanismes que es posen a la disposició dels usuaris per a la seua deguda identificació i autenticació en els sistemes d'informació (claus concertades, contrasenyes, targetes d'identificació, etc.) seran personals i intransferibles.

- Els usuaris són responsables de la custòdia dels mateixos i de tota activitat relacionada amb l'ús del seu accés autoritzat, per la qual cosa no deuran en cap cas revelar o entregar, en cap concepte, els seus mecanismes de credencials d'accés a terceres persones, ni tan sols a altres usuaris o personal al servei de la Diputació de València, ni mantindre-les per escrit a la vista o a l'abast de tercers. Els usuaris no han d'utilitzar cap, accés autoritzat d'un altre usuari, encara que disposen de l'autorització del seu titular.

SEGURETAT EN L'ENTORN DE TREBALL

- Si un usuari té sospites que les seues credencials estan sent utilitzades per una altra persona, ha de procedir immediatament a comunicar la corresponent incidència de seguretat. De la mateixa manera haurà d'actuar-se quan es produïsca la pèrdua o extraviament del mecanisme, un mal funcionament o qualsevol altre comportament anòmal d'aquest.

- Els llocs de treball romandran buidats, sense més material damunt de la taula que el requerit per a l'activitat que s'està realitzant a cada moment. Aquella documentació que no es vaja a utilitzar en el moment haurà de guardar-se en calaixos sota clau o en els armaris o arxivadors corresponents.

- Qualsevol usuari que s'absente temporalment del seu lloc de treball haurà de bloquejar la sessió del seu ordinador (estalvis de pantalla amb contrasenya, etc.) per a impedir l'accés d'altres persones a la informació i a l'equip informàtic. S'establiran bloquejos de sessió automàtics per temps d'inactivitat, requerint una nova autenticació de l'usuari per a reprendre l'activitat en curs.

- Al final de la jornada de treball els usuaris hauran d'assegurar-se que l'equip està apagat i que no es deixa accessible documentació ni suports d'informació de cap mena.

- Quan s'utilitzen pissarres i *flipcharts* els usuaris hauran d'assegurar-se que es netegen adequadament, perquè no quede cap mena d'informació a la vista, abans d'abandonar les sales o despatxos on se situen o permetre que algú alié entre.

- El menjar i beguda poden danyar tant els components electrònics com els suports d'informació, per la qual cosa no hauran de realitzar-se aquestes accions en el lloc de treball, llevat que s'adopten totes les garanties que impedisquen el risc de mal esmentat.

ARXIVADORS I RECINTES DEDICATS A L'EMMAGATZE-MATGE D'INFORMACIÓ

- Els armaris, arxivadors o altres elements en els quals se situen els suports d'informació hauran de disposar de mecanismes de tancament que impedisquen l'accés a persones no autoritzades.
- Sempre que siga possible, aquests armaris o arxivadors han de trobar-se en àrees en les quals l'accés estiga protegit amb portes d'accés dotades de sistemes d'obertura mitjançant clau o un altre dispositiu equivalent. Aquestes àrees hauran de romandre tancades quan no calga l'accés als suports d'informació que contenen.
- Haurà d'evitar-se l'emmagatzematge, depòsit o arxiu de suports d'informació en recintes o armaris d'ús comú, llevat que es garantisca l'existència de mecanismes que facen possible l'accés a la informació únicament al personal autoritzat en cada cas.
- Les dependències destinades a l'arxiu d'informació no s'utilitzaran per a altres usos, com el de magatzem de papereria, d'utensilis informàtics, material de neteja, taquilles i vestidores o qualsevol altra utilitat que supose l'accés a aquests recintes de personal diferent a l'autoritzat per a accedir a la informació emmagatzemada.

INFORMACIÓ EN SUPORTS NO AUTOMATITZATS

- Mentre la documentació no es trobe arxivada, per estar en procés de revisió o tramitació, la persona que es trobe al càrrec de la mateixa haurà de custodiar-la i impedir que puga ser accedida per persona no autoritzada.
- La destrucció dels documents es realitzarà mitjançant màquines destructores, de manera que s'evite la recuperació o reconstrucció de la informació amb posterioritat.
- Sempre que es procedisca al trasllat físic de documents que continguen informació no classificada com a PÚBLICA, hauran d'adoptar-se mesures dirigides a impedir l'accés o manipulació de la informació objecte de trasllat.

"LA SEGURETAT DE LA INFORMACIÓ ÉS UN ESFORÇ CONJUNT, QUE REQUEREIX LA IMPLICACIÓ I PARTICIPACIÓ DE TOTES LES PERSONES USUÀRIES QUE UTILITZEN ELS SISTEMES D'INFORMACIÓ".

MATERIAL COMPLEMENTARI

- "Protecció del lloc de treball", de l'Institut Nacional de Ciberseguretat (INCIBE). Consulta el document en aquest enllaç.
- "Evitant riscos de ciberseguretat en el lloc de treball" d'INCIBE. Consulta la publicació en aquest enllaç.
- "Checklist bàsic per a la protecció del lloc de treball", d'INCIBE. Consulta el checklist en 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.

NOTICIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) ens parla de la privacitat en les reunions en línia.** Les reunions virtuals en línia mitjançant veu, vídeo o a través de serveis web són una constant del treball actual i del teletreball, que s'ha vist enormement potenciat per motiu de la pandèmia de la COVID-19. Si bé cada vegada som més conscients de la necessitat de protegir la nostra privacitat i seguretat en el món en línia, amb les reunions virtuals hem d'adoptar mesures específiques.

  Consulta l'article de l'AEPD en aquest enllaç.

- **El Centre Criptològic Nacional (CCN) emet unes recomanacions per a mètodes d'avaluació i exàmens en remot de manera segura.** El CCN recull les principals mesures a adoptar per a assegurar i preservar la integritat dels mètodes d'avaluació i examen en remot.

  Consulta el document en aquest enllaç.

- **L'Institut Nacional de Ciberseguretat (INCIBE) ens parla de "Bones pràctiques en xarxes socials".** Encara que les xarxes socials poden ser unes eines de gran valor, no podem obviar que moltes vegades són un blanc fàcil per als ciberdelincuentes, aprofitant en moltes ocasions el desconeixement dels perills associats al seu ús per part dels seus administradors. INCIBE ens parla dels riscos que comporta l'ús d'aquestes, per a evitar ser víctimes d'incidents de seguretat.

  Consulta l'article en aquest enllaç.