



Àrea 1 CDD. Compromís professional

Protocol de correu corporatiu

Protocol de correu corporatiu

Dirigit a:

Centres educatius.

Objectiu:

Establir un protocol d'ús del correu corporatiu com eina dins del Pla de Comunicació.

Descripció del recurs:

Aquest recurs permet conèixer totes les funcionalitats del correu corporatiu com les aplicacions per a la gestió del correu, els seus components i també algunes recomanacions en l'ús del correu electrònic, emmagatzematge i seguretat.

Protocol de correu corporatiu

1. Classificació dels comptes de correu d'un centre educatiu	3
2. Aplicacions per a la gestió del correu	4
3. Components del correu electrònic	4
4. Recomanacions en l'ús del correu electrònic	5
5. Bona gestió de l'espai d'emmagatzematge	6
6. Consells de seguretat sobre la utilització del correu	7

Protocol de correu corporatiu

1. Classificació dels comptes de correu d'un centre educatiu

El correu electrònic és un servei de xarxa que permet l'enviament i la recepció de missatges entre diverses parts, sense que totes elles hagen d'estar connectades simultàniament. Per a la comunicació és precís que les parts disposen d'una adreça de correu electrònic. Dins del marc d'actuació de la Conselleria d'Educació s'han creat els següents perfils de treball amb un compte de correu electrònic:

1. IDENTITAT DE CENTRE.

Tots els centres tenen un compte de correu com el següent:

CODICENTRE@edu.gva.es

2. IDENTITAT DEL PERSONAL DOCENT.

Tot el professorat té un compte de correu com el següent:

n.cognom1cognom2N@edu.gva.es

3. IDENTITAT DE L'ALUMNAT.

Tot l'alumnat té un compte de correu com el següent:

nomco1co2N@alu.edu.gva.es

4. IDENTITAT DEL PERSONAL NO DOCENT.

Tot el personal no docent del centre té un compte de correu com el següent:

n.cognom1cognom2N@edu.gva.es

Cal fer la següent consideració, les adreces de correu electrònic de l'alumnat, del personal docent i no docent són dades de caràcter personal i per tant hem de tractar-les segons la llei de protecció de dades.

2. Aplicacions per a la gestió del correu

La gestió del correu electrònic ofert per la Conselleria d'Educació es realitza amb el proveïdor de correu Outlook, que ens permet dues alternatives de treball:

- 1. Client local:** instal·lem en un dispositiu (ordinador, tablet o mòbil) l'aplicació del gestor de correu que necessitem utilitzar i a continuació la configurem per a treballar amb el nostre compte de correu.
- 2. Client Web:** accedim via web al gestor de correu Outlook i a l'iniciar la sessió podem començar a treballar amb el correu. L'avantatge d'esta alternativa és que podem accedir des de qualsevol dispositiu que tinga accés a internet.

3. Components del correu electrònic

Tots els missatges de correu electrònic estan formats per una sèrie d'elements, alguns dels quals són obligatoris, altres són recomanables i uns altres són opcionals.

Elements obligatoris: els únics són l'adreça de correu de la persona emissora, i l'adreça o les adreces de les persones receptores. Les persones receptores poden ser individuals, llistes de contactes o grups. **Elements recomanables:** faciliten la gestió del correu electrònic. Els més importants són:

- L'assumpte o tema del correu.
- El cos del missatge.

Elements opcionals: són variables. Entre ells cap destacar els elements adjunts o la signatura de la persona emissora.

A més de les dades visibles, els missatges de correu electrònic disposen d'altres dades en les seues capçaleres, les quals permeten obtenir informació addicional que podem desar en un arxiu amb el format eml. Cal tindre en compte que algunes d'aquestes capçaleres poden ser considerades com a dades de caràcter personal. Entre aquestes dades cap fer menció de l'adreça IP de la persona emissora o la data i l'hora de l'enviament.

4. Recomanacions en l'ús del correu electrònic

A continuació, anem a indicar una sèrie de recomanacions i bons consells a l'hora de fer servir el correu:

1. Emplenar sempre el camp de l'assumpte amb un text resum del contingut i amb paraules clau que ens permeten la seua classificació mitjançant les regles que proporciona el gestor de correu.
2. Quan necessitem enviar un correu a una llista de contactes o a un grup nombrós de contactes és convenient escriure les seues adreces de correu dins del camp C/o (Còpia Oculta) per dos motius, primer, per ocultar a la resta de destinataris l'adreça de correu de cadascú d'ells i així complir amb la llei de protecció de dades (l'adreça de correu és considerada una dada personal) i segon, per a evitar que els spammers puguen aconseguir adreces de correu legítimes per a fer les campanyes de spam.
3. Si enviem un arxiu adjunt és convenient que siga un enllaç a la seua ubicació en el Sharepoint, d'esta forma evitem incrementar l'espai d'emmagatzematge en totes les còpies que poden generar-se per a cada destinatari, a més, en cas que fem modificacions sobre este arxiu apareixerà actualitzat per a totes les persones que han rebut l'enllaç i així evitem enviar un altre correu amb les modificacions realitzades sobre l'arxiu. En cas d'enviar l'arxiu adjunt a persones que no disposen de la identitat digital podríem fer-ho mitjançant un vincle públic a la seua ubicació dins del Sharepoint de l'equip Documentar.
4. Configurar el correu amb un peu de signatura que continga la imatge corporativa i que aparega en tots els correus de sortida, tal com es veu a continuació

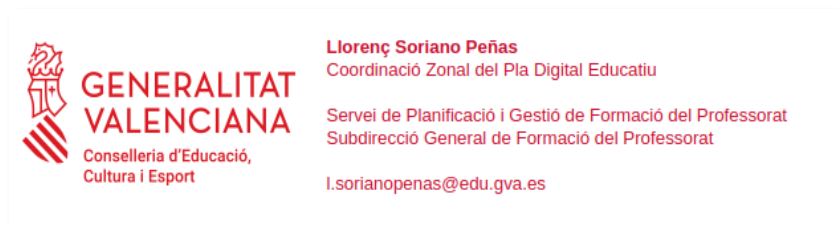


Figura 1: "Peu de signatura amb la imatge corporativa"

5. Bona gestió de l'espai d'emmagatzematge

Les bústies associades a les identitats digitals tenen una gran capacitat d'emmagatzematge d'informació, és igual a 50 GB, que pot pareixer més que suficient, però amb l'ús del correu podem arribar al seu límit, i en aixe cas, no podrem enviar i rebre correus electrònics associats a la nostra identitat digital. Per aquest motiu, volem exposar els següents consells sobre la seua gestió:

- Consultar l'espai utilitzat per a emmagatzemar els correus:
 - Dins de la configuració de l'Outlook cal obrir l'opció de "Mostrar tota la configuració de l'Outlook".



Figura 2: "Opció del menú de configuració de l'Outlook"

- Dins de la configuració "Generals" cal seleccionar l'opció "Emmagatzematge".

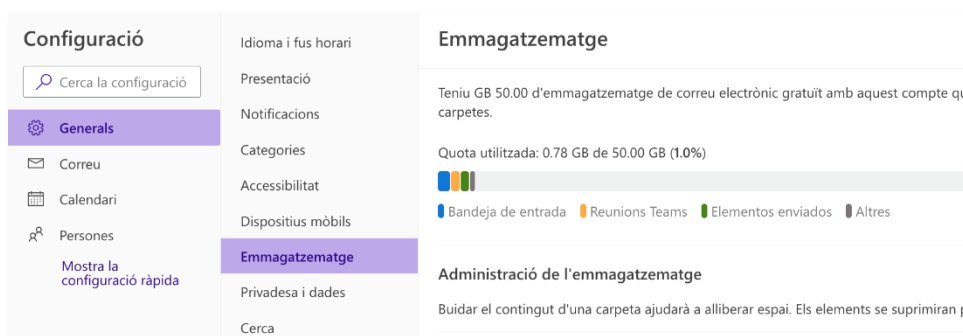


Figura 3: "Pantalla de configuració amb l'Opció Generals, Emmagatzematge"

Podem visualitzar la distribució de l'espai d'emmagatzematge entre les diferents carpetes creades amb la possibilitat de poder esborrar total o parcialment el seu contingut.

- Buidar les carpetes de correu:

Podem eliminar el contingut de les carpetes en funció de l'antiguitat dels correus o directament esborrar tot el contingut. Hem de considerar que els missatges que eliminem d'esta manera desapareixeran definitivament, i per tant, no es podran recuperar.

6. Consells de seguretat sobre la utilització del correu

El correu electrònic és un dels vectors d'atac preferits per la ciberdelinqüència. Molts dels atacs que es produeixen contra persones i contra empreses comencen amb la recepció d'un missatge de correu amb una càrrega de malware. Tot i que els sistemes de la Conselleria estan protegits, resulta molt convenient seguir una sèrie de pautes que ajuden a incrementar la protecció de les persones usuàries del servei.

Algunes de les qüestions a tindre en compte relatives a la seguretat i la protecció de les dades són les següents:

- 1.** Identificar el phishing dins del nostre correu en base als següents indicis:
 1. Sol·licituds d'informació personal per part de persones o empreses que mai les han de sol·licitar per aquest mitjà (banca, administració, ...).
 2. Errors sintàctics i gramaticals. Moltes vegades hi ha expressions o formes d'escriure que indiquen que es tracta d'un missatge fraudulent.
 3. Comunicacions on s'informa que s'ha guanyat algun tipus de premi, regal o gratificació que no s'espera.
 4. Contenen enllaços o arxius adjunts sospitosos.
 5. Els noms de domini de les adreces o dels enllaços no són coherents.
- 2.** No s'ha de respondre mai als correus sospitosos ni interactuar amb els elements que puguen estos missatges, com per exemple enllaços o formularis. Tampoc s'ha de descarregar ni obrir els arxius adjunts que els acompanyen.
- 3.** Informar sobre els correus sospitosos i/o no desitjats:

1. Els clients de correu electrònic inclouen l'opció d'informar sobre correu brossa i sobre correus de phishing. Esta pràctica ajuda a millorar el sistema de protecció de tota la corporació. En aquest sentit, podem trobar a la barra d'eines de l'Outlook web el botó "Informa" per a traslladar aquesta informació.

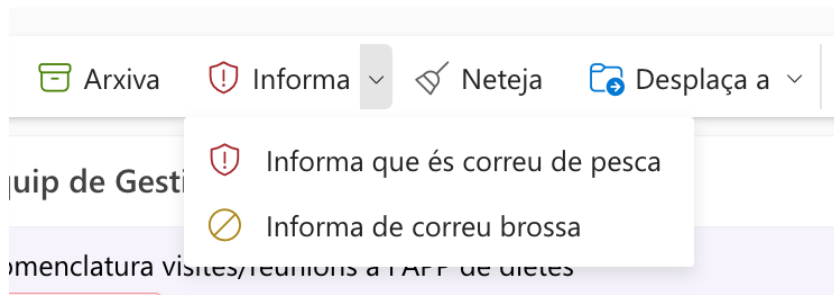


Figura 4: "Menú que inclou l'opció d'informar sobre correu brossa i correu de phishing"

No compartir informació de caràcter personal i d'esta manera impedim que arribe a destinataris no desitjats.

4. Utilitzar contrasenyes segures i canviar-les regularment.

A continuació, mostrem una infografia de l'INCIBE sobre com identificar un correu electrònic maliciós:



Figura 5: "Cómo identificar un correo electrónico malicioso" INCIBE. OSI, Oficina de Seguridad del Internauta. <https://www.osi.es/es/como-identificar-un-correo-electronico-malicioso>. Licència Copyright.

El recurs **Protocol de correu corporatiu** ha sigut creat per :

Equip del Pla Digital Educatiu

Subdirecció General de Formació del Professorat

Secretaria Autonòmica d'Educació i Formació Professional

Conselleria d'Educació, Cultura i Esport



Aquesta obra està sota una [Llicència Creative Commons Atribució-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

Material de suport per als centres educatius de la Comunitat Valenciana,
març 2023