

Tot el que has de saber de seguretat informàtica

Conferència a càrrec de
Enric Font

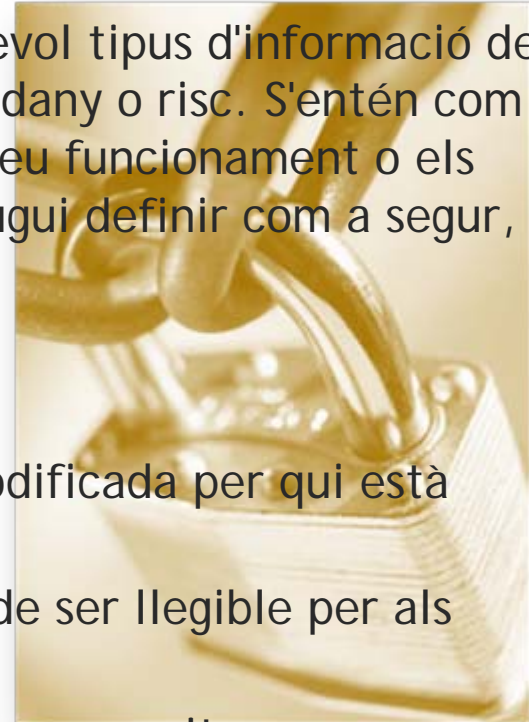
Introducció

La seguretat informàtica consisteix a assegurar que els recursos informàtics d'una organització siguin utilitzats d'una manera segura i fiable, i que l'accés a la informació, així com la seva modificació, només sigui possible a les persones que estiguin acreditades i dins dels límits de la seva autorització.



Introducció

- Un sistema segur és aquell en el que qualsevol tipus d'informació de la nostra empresa es troba lliure de perill, dany o risc. S'entén com a perill o dany tot el que pugui afectar el seu funcionament o els seus resultats. Per tal que un sistema es pugui definir com a segur, ha de complir tres característiques:
- **Integritat:** La informació només pot ser modificada per qui està autoritzat i de manera controlada.
- **Confidencialitat:** La informació només ha de ser llegible per als autoritzats.
- **Disponibilitat:** Ha d'estar disponible quan es necessita.



Escola Seguretat



Política de Seguretat Informació

És un conjunt de normes, directrius i protocols a seguir, on es defineixen les mesures a prendre per a protegir la seguretat del sistema. Una bona regla es: “El que no es permet expressament, està prohibit”, és a dir, l’empresa proporciona uns permisos ben determinats i documentats, y qualsevol altra cosa està prohibida.”

Els actius que la seguretat informàtica té com a objectiu protegir són :

- **Informació.** És el actiu de més valor per a l’empresa.
- **Equips.** Maquinari i Programari.
- **Usuaris.** Persones que utilitzen els sistemes informàtics i manegen la informació.



Avaluació de Riscos i Amenaces

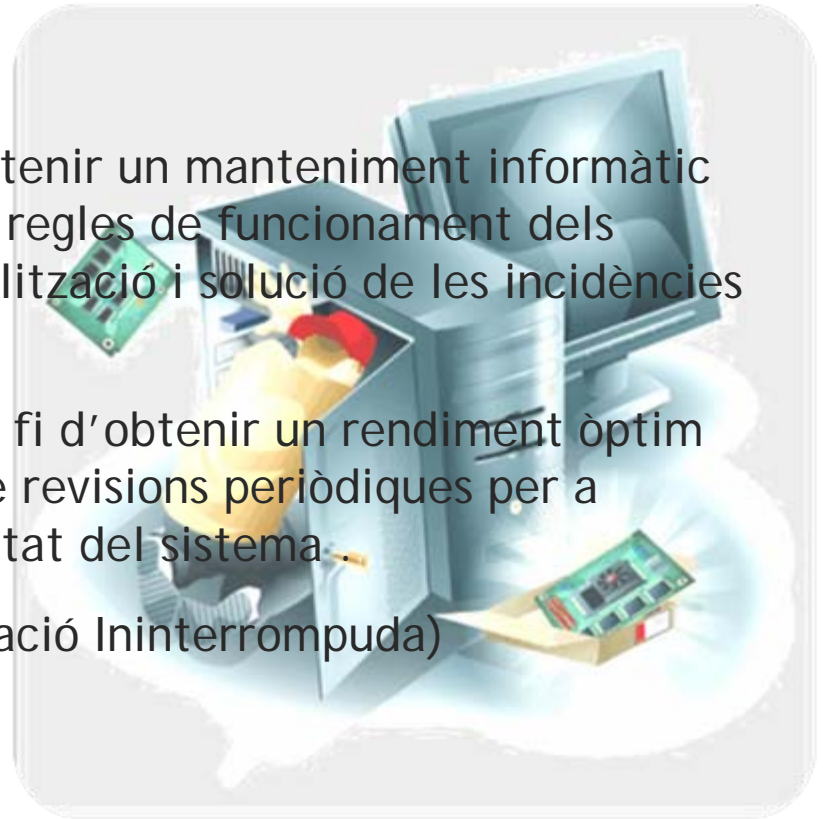
- Cal calcular quines amenaces i riscos hi ha, i la probabilitat que succeeixin cadascun d'ells, per poder prioritzar el pla de seguretat.
- L'avaluació econòmica de l'impacte d'aquest successos, ens servirà per contrastar el cost de la protecció de la informació en comparació al cost de tornar-la a produir.
- Preguntes que ens hauríem de contestar:

- ✓ Què pot anar malament?
- ✓ Amb quina freqüència?
- ✓ Quines serien les conseqüències?
- ✓ Quin es el cost d'una hora, un dia... sense treballar?
- ✓ Quina és la informació confidencial o sensible?
- ✓ Com s'actuarà si la seguretat és violada?

Tipus de risc	Factor
Robament informació	Alt
Virus	Alt
Error usuari	Mig
Error maquinari	Baix
Accessos no autoritzats	Baix
Foc, inundacions etc..	Molt baix

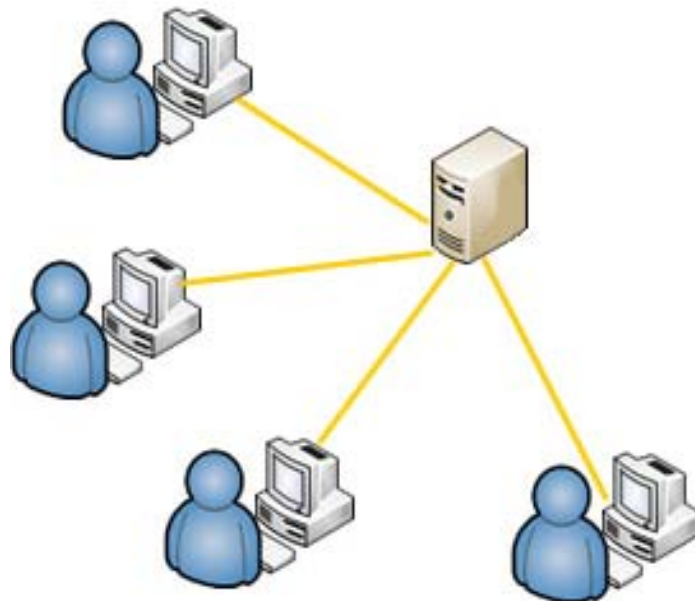
Maquinari

- **Directives del sistema:** Per obtenir un manteniment informàtic estable, cal crear una sèrie de regles de funcionament dels terminals que permetin la localització i solució de les incidències dels usuaris.
- **Optimitzacions del sistema:** A fi d'obtenir un rendiment òptim del sistema, cal portar a terme revisions periòdiques per a verificar i actualitzar la integritat del sistema.
- **Usar SAI'S(Sistemes d'Alimentació Ininterrompuda)**



Identificació

- Usuaris locals identificats i amb accés amb contrasenya.
- Servidor central amb tota la informació compartida, amb política de permisos i autenticació d'usuaris
- Evitar contrasenyes fàcils (admin, 1234 etc...)
- Canvis periòdics de contrasenyes



Protecció Local

Un **virus informàtic** és un programa que es copia automàticament i altera el funcionament normal de l'ordinador, sense el permís o el coneixement de l'usuari.

Els virus informàtics tenen, bàsicament, la funció de propagar-se, replicant-se, però alguns contenen a més instruccions perjudicials amb diferents objectius, des de fer una simple broma fins a produir danys importants en els sistemes, o bloquejar les xarxes informàtiques generant tràfic inútil.

Antivirus Gratuïts:

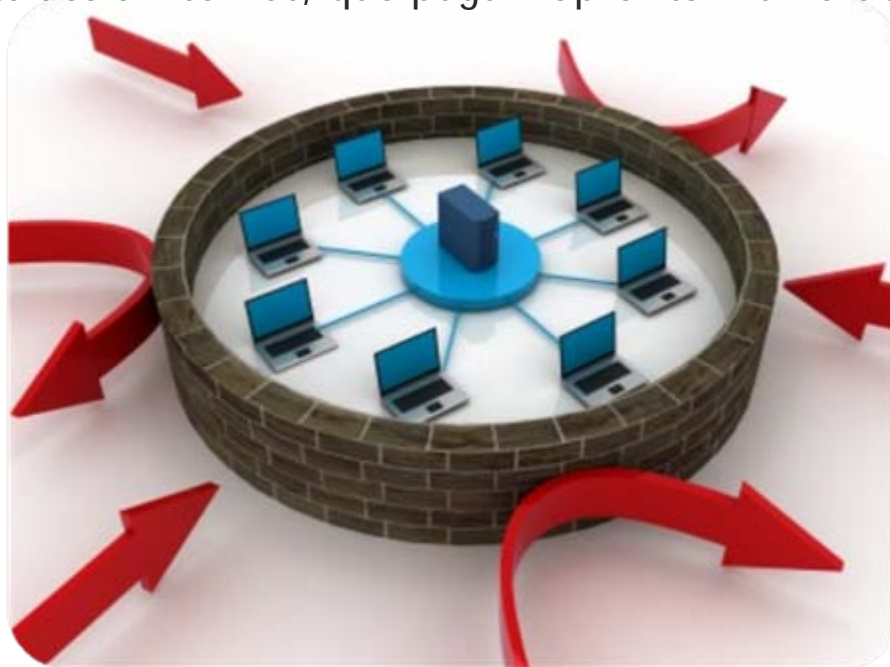
- AVG Anti-Virus <http://free.avg.com/es-es/inicio>
- BitDefender <http://www.bitdefender.es/site/Downloads/>
- Avast <http://www.avast.com/es-es/index>
- Avira Antivir <http://www.antivir.es/cms/>
- <http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&displaylang=es>

Amenaces

- **Phising:** suplantar identitat d'una empresa (gen. per correu)
- **Pharming:** redireccionament de domini quan naveguem per internet.
- **Keylogger:** software o hardware que registre pulsacions de tecles, les emmagatzema i envia per internet.
- **Hoax:** rumors falsos (per correu).
- **Adware:** Publicitat no desitjada quan naveguem per internet
- **Spam:** correu brossa.
- **Scam:** estafa, per correu o en webs que venen productes que no s'entreguen.
- **Dialer:** software que marca un número de telèfon de tarificació especial (906) des del mòdem (no cable ni adsl).
- **Spyware:** recopila informació sobre activitats, contrasenyes...

Protecció Perimetral

- Un tallafocs (firewall en anglès), és un element de maquinari o programari utilitzat en una xarxa per controlar les comunicacions, permetent-les o prohibint-les segons les polítiques de xarxa que hagi definit l'organització. La ubicació habitual d'un tallafocs és el punt de connexió de la xarxa interna de l'organització amb la xarxa exterior, que normalment és Internet; d'aquesta manera es protegeix la xarxa interna d'intents d'accés no autoritzats des d'Internet, que puguin aprofitar vulnerabilitats.



Firewalls gratuïts

- **ZoneAlarm** <http://www.zonealarm.com>
Servidor bàsic de seguretat, que ofereix una protecció fiable contra intents de intrusió. Proporciona protecció a diferents nivells.



- **Outpost Firewall Free** <http://www.outpost-es.com/home/index.html>
Potent firewall, fa servir la tecnologia basada en plug-ins que es un sistema de tasques per detectar intrusos, filtres, vigilància del correu electrònic, bloqueig antispam (elimina banners i popups) i control de privacitat.



- **PC Tools Firewall** <http://www.pctools.com/es/>
Firewall ple de funcions i fàcil d'usar.



Copies Seguretat

Una **còpia de seguretat** (*backup* en anglès) fa referència a la còpia d'informació que es realitza per tal de ser restaurada en cas de pèrdua de dades o en cas de ser requerida en posterioritat.

Normalment les dades es copien en un mitjà d'emmagatzemament **diferent** al de l'origen de les dades, com poden ser: discos durs externs, DVD, cintes magnètiques (DAT), etc. Cada cop s'utilitzen més sistemes de còpia de seguretat remota que realitzen les còpies de forma automàtica a través de la xarxa.

Planificació de les còpies de seguretat

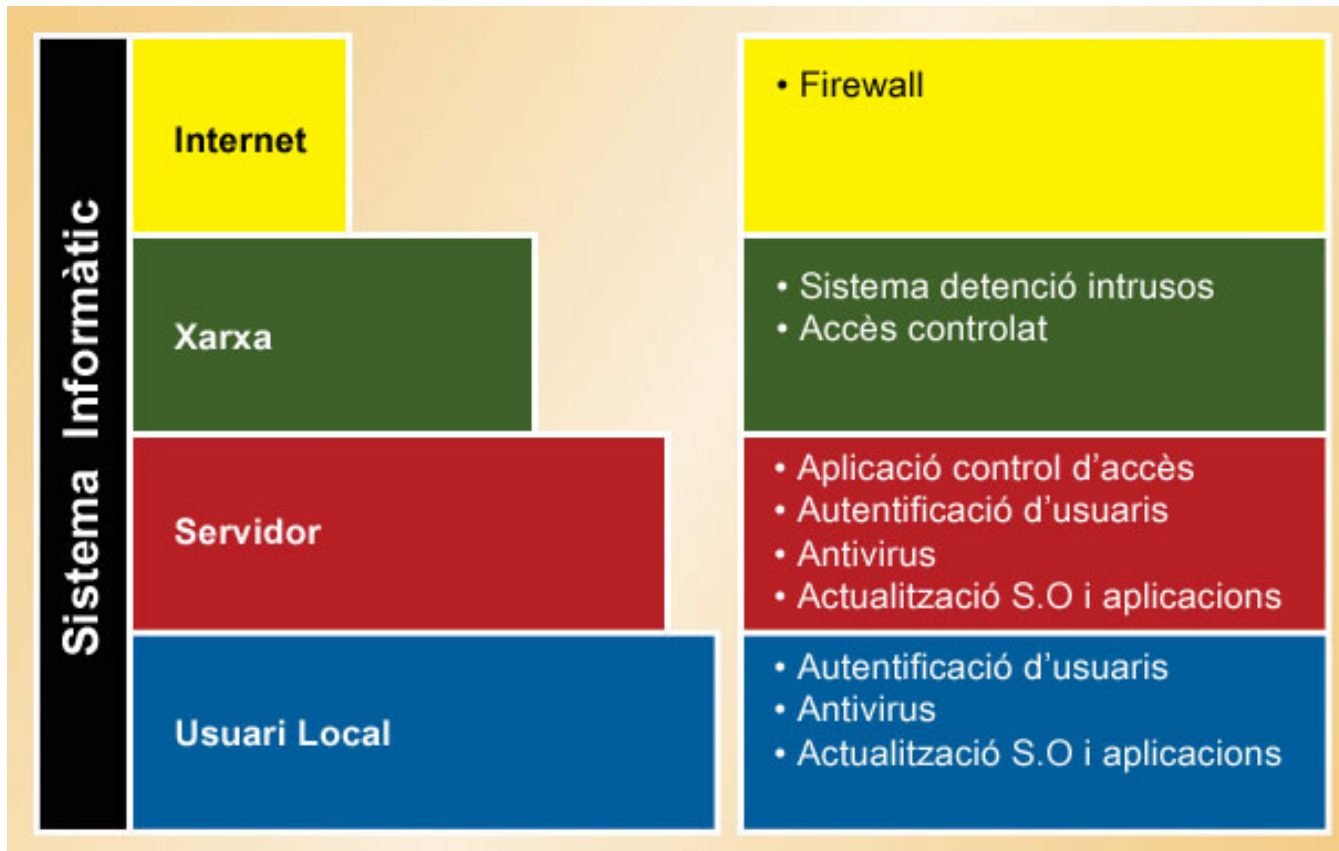
- El volum de dades a copiar
- El cost econòmic dels mitjans d'emmagatzemament
- L'operativitat de la solució escollida tant pel que fa al temps de còpia com el de recuperació.
- La periodicitat de les còpies. Com més alta la freqüència major capacitat de recuperació es tindrà.
- El número de còpies. Si es realitza més d'una còpia i aquestes desen en ubicacions separades s'augmentarà la seguretat.



Seguretat Wifi

- La tecnologia WiFi en els seus diferents estàndards utilitza freqüències per a transmetre de 2,4 o 5 GHz. Aquestes freqüències són freqüències no llicenciades per la Comissió Nacional de Comunicacions (CNC), el que equival que no requereixen cap tipus de llicència especial per a operar. Com la tecnologia 802.11 és lliure, podem trobar-nos amb que altres usuaris o empreses estiguin operant a les proximitats del nostre sistema, amb les lògiques interferències en la transmissió de dades del nostre sistema. Per això els propis sistemes ofereixen solucions de seguretat eficaces per a evitar interferències i escoltes a les nostres comunicacions.
- Per a començar, els productes sense fil contenen amb 14 canals de freqüències seleccionables dins de les bandes No Llicenciades, la qual cosa permet escollir un canal lliure d'interferències a l'hora d'instal·lar el nostre sistema. D'altra banda, els productes ofereixen Codis d'Encriptació (Wireless Encryption Protocol o WEP), encriptant les dades amb claus de 40 o 128 bits.

Resum Protecció



Manteniment bàsic de l'ordinador

- Antivirus: Cal tenir-lo configurat amb actualitzacions automàtiques.
- Antiespies: Aplicacions que esborren programari malintencionat.
- Firewall: No permet que altres sistemes o ordinadors de la xarxa puguin accedir a la nostra xarxa.
- Scandisk: Verifica l'estat físic dels discs magnètics de l'ordinador i en permet reparar els fragments defectuosos.
- Compactador: Reorganitza els fitxers dels discos magnètics de l'ordinador agrupant-los per optimitzar-ne l'ús. Llavors el sistema anirà més de pressa i desarà els fitxers nous amb més eficàcia.
- Còpia de seguretat: a un altre dispositiu la informació de tots els discs durs.
- Restauració del sistema: Opció que us ofereix la possibilitat de deixar el vostre PC tal i com el teniu configurat i amb el programari d'un dia determinat.
- Neteja del disc: Esborra els fitxers que ocupen espai, i que no són necessaris per al funcionament del vostre PC (paperera, catxé del navegador, cookies, ...)
- Ccleaner: Programa gratuït de neteja del disc. www.ccleaner.com
- Instal·lar totes les actualitzacions del S.O

Per què va lent l'ordinador

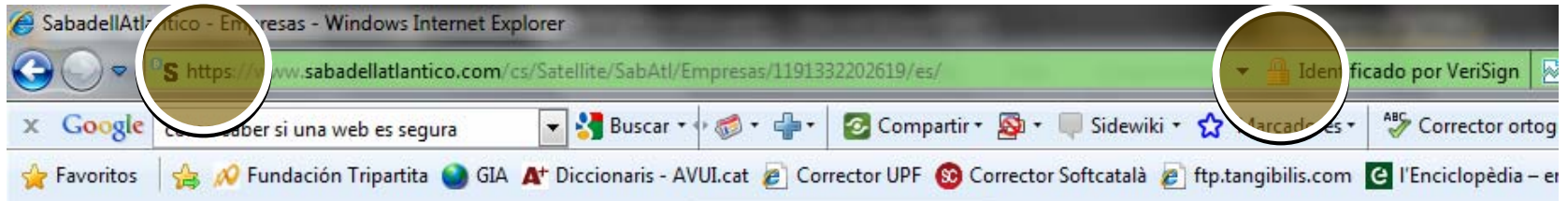
Pot haver-hi múltiples raons. Les principals són que el maquinari ja no és suficient o que el programari de l'equip està fallant per alguna d'aquestes causes:

- Els virus, Malware, Spyware etc.
- La gran quantitat de programes residents a la memòria del nostre ordinador.
- La incorrecta des instal·lació del programari.



Identificar webs segures

- Certificat SSL. Ens dona la seguretat que la informació que enviarem a través d'Internet viatjarà encriptada i no podrà ser descryptada per una tercera persona.

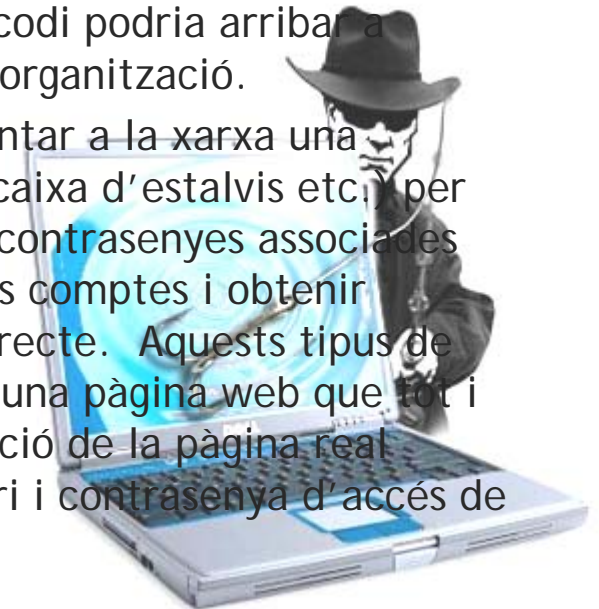


- Si cliquem damunt del candau groc, ens donarà informació sobre el certificat SSL

Google te una útil eina que permet examinar qualsevol domini para comprovar si la web es segura. Només cal afegir el domini a aquesta adreça:
<http://www.google.com/safebrowsing/diagnostic?site=www.tangibilis.com>

Gestionar de forma segura el correu

- **Spam.** Recepció de grans volums de correu electrònic no desitjat a les bústies professionals dels usuaris que ocupen espai del servidor de correu electrònic inútilment, i consumeixen temps de l'usuari a l'hora d'eliminar-los de la seva bústia de correu.
http://www.spamfighter.com/Lang_ES/Anti_spam_software.asp
- **Infecció per codi maliciós.** Els fitxers adjunts als correus electrònics poden estar infectats per codi maliciós. Aquest tipus de codi podria arribar a paraitzar la infraestructura informàtica de tota l'organització.
- **Phising.** Pràctica delictiva que consisteix en suplantar a la xarxa una empresa de confiança (normalment un banc, una caixa d'estalvis etc.) per tal d'apropiar-se dels identificadors d'usuari i les contrasenyes associades dels seus clients on-line i així poder entrar als seus comptes i obtenir informació confidencial o un benefici econòmic directe. Aquests tipus de missatges acostumen a incorporar un enllaç cap a una pàgina web que tot i que sembla una pàgina web legítima, és una imitació de la pàgina real mitjançant la qual es roben l'identificador d'usuari i contrasenya d'accés de la víctima.



Recomanacions

- Sempre que sigui possible, és millor enviar correus electrònics que no continguin documents adjunts, incorporant la informació al cos del missatge i no en un fitxer independent.
- En el "Tema", cal escriure una frase que ajudi al receptor a saber de què tracta el missatge, i li permeti filtrar-lo, prioritzar-lo, arxivar-lo i més endavant recuperar-lo.
- No obrir missatges de correu electrònic i encara menys fitxers adjunts en els supòsits que es descriuen a continuació. Esborrar aquests missatges sense obrir-los i, a continuació, eliminar-los de la paperera.
 - Es desconeix qui és el remitent del missatge,
 - Si el títol del missatge no indica quin és el motiu del missatge,
 - Si el missatge és inesperat o per algun motiu es considera que és estrany, independentment de qui sigui l'emissor. Possiblement es tracta de spam o són missatges generats per virus o altre codi maliciós.
- No obrir mai fitxers adjunts executables.



Recomanacions

- No contestar mai missatges de correu brossa, ni respondre a l'opció de "donar de baixa la subscripció" d'aquests missatges, per evitar donar a conèixer als emissors d'aquest tipus de correus que es tracta d'una adreça de correu vàlida, i evitar així que pugin intensificar l'enviament de correu brossa.
- Mai respondre sol·licituds de claus que arribin mitjançant el correu electrònic. Desconfii de qualsevol petició de dades personals i mai proporcioni informació personal o financera en resposta a un correu electrònic, ni utilitzi enllaços incorporats en aquests correus electrònics o en pàgines web de tercers.
- Desactivar la funció de "vista prèvia" als clients de correu electrònic (Outlook, Thunderbird, Eudora, Lotus Notes, etc.), per evitar infeccions víriques.

Organitza



Amb el suport



Llicència de Creative Commons

Aquest document està subjecte a una llicència de
Reconeixement - No comercial
Sense obres derivades 3.0 - Espanya - de Creative Commons

