#AprenemCiberseguretat

SEGURETAT DE LA INFORMACIÓ

EL **ROBATORI D'INFORMACIÓ DIGITAL ÉS LA SOSTRACCIÓ IL·LEGAL DE DADES EMMAGATZEMADES** EN ORDINADORS, SERVIDORS O ALTRES DISPOSITIUS D'UNA VÍCTIMA AMB LA INTENCIÓ DE COMPROMETRE LA SEUA PRIVACITAT O OBTENIR INFORMACIÓ CONFIDENCIAL.
DAVANT AQUEST RISC ÉS RECOMANABLE L'ENCRIPTACIÓ D'INFORMACIÓ, LES CÒPIES DE SEGURETAT I L'ESBORRAMENT SEGUR.

ENCRIPTACIÓ D'INFORMACIÓ

Mètode pel qual **convertim en il·legible** una determinada informació o missatge perquè només hi accedisca la persona autoritzada fent ús d'una contrasenya, codi o PIN necessari per a desxifrar-lo.

Encriptació simètrica. Les dues parts coneixen la clau d'encriptació. És la mateixa clau necessària per a la desencriptació.

Encriptació asimètrica. Utilitzen dues claus que modifiquen un missatge digital i el fan il·legible. Només pot ser llegit per qui posseïsca les dues claus.

EINES D'ENCRIPTACIÓ SEGURA

- BitLocker
- VeraCrypt
- BoxCryptor
- BitLocker
- VeraCrypt
- BoxCryptor
- Enigmail
- HTTPS Everywhere

CÒPIES DE SEGURETAT

Procés mitjançant el qual es **duplica la informació existent d'un suport a un altre.** La finalitat és poder recuperar les dades contingudes en cas de fallada del primer suport d'allotjament.

BONES PRÀCTIQUES

1. Utilitzeu les còpies de seguretat en dos nivells. Dues còpies de seguretat per a arxius més importants.
2. Feu la **còpia de seguretat periòdicament**.
3. **Encripteu** les vostres còpies de seguretat.
4. Useu **programari dedicat** per a fer les còpies de seguretat.

REALITZAR CÒPIES DE SEGURETAT EN LA UV

La Universitat de València posa a la nostra disposició dos serveis que realitzen còpies de seguretat periòdiques:

disco.uv.es
nuvol.uv.es

Garanteixen la seguretat amb un **sistema de còpies centralitzades**.

ESBORRAMENT SEGUR

Mètode **d'esborrament d'arxius** que es caracteritza per sobreescriure les dades amb el propòsit d'impedir la seua recuperació. Això és aplicable tant per a informació en format físic com digital.

MÈTODES D'ESBORRAMENT SEGUR

SÍ

1. DESMAGNETITZACIÓ. Permet destruir de manera permanent els dispositius d'emmagatzematge magnètics i, per tant, la informació que contenen.
2. DESTRUCCIÓ FÍSICA. Desintegració, polvorització, fusió i incineració. El seu objectiu és destruir el suport d'emmagatzematge.
3. SOBREESCRIPTURA. S'ha d'escriure la totalitat de la superfície d'emmagatzematge per assegurar la total destrucció de les dades.

NO

1. COMANDOS D'ESBORRAMENT DEL SISTEMA OPERATIU. Accedeixen a la "llista d'arxius" i marquen l'arxiu com a suprimit, però el seu contingut continua intacte.
2. FORMATACIÓ D'UN DISPOSITIU. Se sobreescriu l'àrea destinada a la "llista d'arxius" sense que l'àrea de dades on es troba el contingut dels arxius haja sigut alterada.

ESBORRAMENT D'EQUIPS EN LA UV

USUARI/ÀRIA - Persona encarregada de realitzar un esborrament segur dels equips.

ELEMENTS DE L'EQUIP A ESBORRAR:

- usuari amb accés a l'equip;
- documents generats per l'usuari/ària;
- directoris i/o carpetes de l'equip/suport.

Si l'usuari/ària no disposa dels coneixements suficients per a dur a terme aquestes accions, **posar-se en contacte amb el CAU** per a realitzar l'esborrament segur de l'equip.

WWW.UV.ES/UVSTIC

VNIVERSITAT DE VALÈNCIA
UVstic
Vicerectorat d'Estratègia, Qualitat i Tecnologies de la informació
Conscienciació en la seguretat de la informació