Novembre de 2022

CONSCIENCIACIÓ EN CIBERSEGURETAT

SEGURETAT FÍSICA I LÒGICA

Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

1. Seguretat física i lògica: dos conceptes CONVERGENTS en la seguretat de la informació

El **Pla de Seguretat de la Informació** d'una organització haurà de descriure com s'implementa la seguretat en aquesta organització, així com quines són les polítiques que es defineixen, els seus controls i solucions.

Aquest Pla de Seguretat es desenvoluparà considerant **tots els recursos de TI en funció dels nivells de seguretat aconseguits** i haurà de centrar-se en les accions necessàries per tal d'aconseguir els nivells més alts de seguretat.

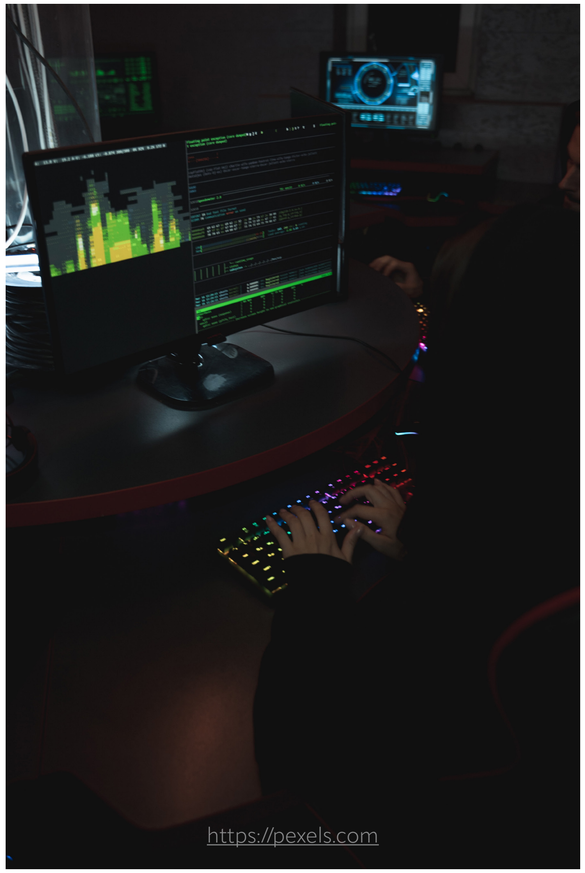
La Seguretat Física i Lògica són **dos aspectes claus** en un Pla de Seguretat de la Informació i són necessaris per implementar la seguretat en les organitzacions.

Habitualment, ens centrem a protegir-nos de possibles *hackers*, virus, *ransomwares*... i ens oblidem d'un aspecte molt important en la Seguretat de la Informació: la **Seguretat Física i Lògica**.

La **Seguretat Física** és aquella que tracta de **protegir el *hardware* dels equips i el seu cablejat** dels possibles desastres naturals que poguessin produir-se (terratrèmols, tifons, huracans, incendis, inundacions, sobrecàrregues elèctriques), així com d'una infinitat més d'amenaces que poguessin donar-se lloc.

La **Seguretat Lògica** complementa a la Seguretat Física, ja que aquesta **protegeix el *software* dels equips informàtics**. És a dir, **les aplicacions i les dades** d'accions realitzades per part dels usuaris, així com de robatoris, pèrdues de dades, entrades de virus informàtics, modificacions no autoritzades, atacs des de la xarxa, etc.

Per tant, són dos conceptes que **convergeixen entre si** i van donats de la mà.


https://pexels.com

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

2.1. Mesures de Segureta Físiques:
a) Àrees segures

https://stock.adobe.com

1. Mesures de Seguretat establertes per a protegir el perímetre de Seguretat Física de l'organització:

- Els **perímetres de les zones** on es trobi l'organització han de tenir una consistència sòlida que eviti l'existència de bretxes de seguretat.
- Les **parets, sòls i sostres** han de tenir la consistència requerida, segons la zona, per a evitar els accessos no autoritzats.
- El perímetre ha de comptar amb un **sistema de videovigilància**.
- Les **portes** han de disposar de **mecanismes de control d'accés físic**.
- El **personal extern** sol pot **accedir a l'edifici a través de la recepció i estar per a això degudament identificat**.

2. Mesures de Seguretat establertes per a garantir la seguretat en les oficines, despatxos i altres recursos

- Les **instal·lacions clau** hauran de situar-se de manera que s'eviti l'accés per part del públic.
- La **senyalització d'edificis** haurà de ser la **mínima imprescindible**, evitant donar indicacions de les activitats.
- Les **instal·lacions** hauran de configurar-se per a evitar que **la informació confidencial** emmagatzemada a l'interior pugui ser visible o audible.

3. Mesures de Seguretat per a protegir l'organització de possibles amenaces externes i mediambientals

- Les **barreres físiques i elements de prevenció, detecció i extinció** hauran de complir amb el que s'estableix en la Llei de Prevenció de Riscos Laborals.
- S'hauran d'analitzar els **riscos de danys provocats per amenaces externes i d'origen ambiental** (incendis, inundacions, terratrèmols, etc.).

2.1. Mesures de Seguretat Físiques: b) Seguretat dels èquips informàtics

https://es.Vecteezy.com

1. **Mesures de Seguretat imposades en els equips informàtics:**
   - Els sistemes se situaran de tal manera que es **minimitzin els accessos innecessaris**.
   - Els **equips de tractament i emmagatzematge d'informació** s'instal·laran de tal manera perquè **es redueixi el risc** de que la informació sigui accessible per persones no autoritzades.
   - Les **diferents ubicacions dels sistemes** hauran de comptar amb controls per a minimitzar els possibles riscos i amenaces d'origen natural. No es permetrà **l'accés als CPD's amb aliments, substàncies o líquids** que puguin provocar incidents en aquests.

2. **Mesures de Seguretat imposades en les instal·lacions de subministraments de l'organització:**
   - Els sistemes hauran de comptar amb **elements de comunicacions redundants**, així com múltiples proveïdors de telecomunicacions.
   - El **subministrament als sistemes crítics** es trobarà controlat i recolzat per sistemes d'alimentació ininterromputs d'aire. Es trobaran degudament definits els **procediments d'actuació davant incidents de seguretat** relacionats amb els subministraments.

3. **Mesures de Seguretat per a la protecció del cablejat de les instal·lacions:**
   - El **cablejat** de qualsevol classe es realitzarà mitjançant **canalons localitzats en sòls i/o sostres tècnics** que serveixin per dificultar l'accés no autoritzat.
   - Els **cables, equips de telecomunicacions** i alimentació estaran degudament **identificats, etiquetats i llistats** per tal d'evitar errors en la gestió o manipulació d'aquests.
   - **Els quadres elèctrics, dispositius de comunicacions i els *patch panel* de planta** es trobaran a l'interior d'armaris tancats.

2.1. Mesures de Segureta Físiques:
b) Seguretat dels èquips informàtics (continuació)

https://stock.adobe.com

4. Mesures de Seguretat imposades en els equips i actius desplaçats fora de les instal·lacions de l'organització:

- S'hauran **d'avaluar i tractar els riscos** que pogués suposar tenir equips informàtics fora de les instal·lacions.
- Els equips i suports de dades que es trobin fora de les instal·lacions de l'organització **no es podran deixar desatesos en llocs públics**.
- Es respectaran les instruccions del fabricador relatives a la **conservació i protecció dels equips** enfront d'amenaces externes.

5. Mesures de Seguretat imposades durant la utilització/retirada segura de dispositius d'emmagatzematge

- Els **suports d'informació** que puguin ser reutilitzats seran degudament esborrats, mitjançant **l'aplicació de procediments tècnics d'esborrat segur** per a garantir que la informació no pugui ser recuperada.
- Els sistemes i suports que no vagin a ser reutilitzats o en els quals no pogués garantir-se un **esborrat segur** hauran de ser **destruïts degudament**, seguint la normativa d'eliminació de suports.

6. Mesures de Seguretat establertes en els llocs de treball

- Quan s'abandona el lloc de treball, **les taules hauran d'estar lliures de documents confidencials**.
- Els **llocs d'usuari quedaran degudament bloquejats**, evitant mostrar cap informació.
- Els **documents impresos seran recollits immediatament després del seu enviament i guardats** en llocs segurs.
- El **material utilitzat pels empleats es guardarà en llocs tancats**, com a calaixeres o armaris amb pany.

3. Mesures de Seguretat Lògica

La **SEGURETAT LÒGICA** es refereix als controls específics establerts per a administrar l'accés als sistemes informàtics.

Les **contrasenyes i els perfils d'usuari** són un enfocament comú per a restringir l'accés, assegurant que només el **personal autoritzat pugui accedir als sistemes clau**, per exemple: els servidors.

Per tant, la Seguretat Lògica ajuda a **protegir contra amenaces conegudes com a atacs cibernètics**.

Els **principals objectius** d'aquests controls de Seguretat Lògica són els següents:

- Limitar l'accés als programes i arxius.
- Assegurar l'ús de programes, arxius i dades correctes i pels mitjans adequats.
- Que la informació compartida es rebi només pel destinatari al qual s'ha enviat i no a un altre.
- Creació de sistemes d'emergència alternatius per a transmetre informació.

Exemples de Mecanismes de Defensa per garantir la Seguretat Lògica

Amenaces	Mecanismes de defensa
Robatoris	• Xifrar la informació emmagatzemada en els suports perquè en cas de robatori no sigui llegible. • Utilitzar contrasenyes per a evitar l'accés a la informació. • Sistemes biomètrics (ús d'empremta dactilar, targetes identificadores, cal·ligrafia...).
Pèrdua de la informació	• Realitzar còpies de seguretat per a poder restaurar la informació perduda. • Ús de sistemes tolerants a fallades, elecció del sistema de fitxers del sistema operatiu adequat. • Ús de conjunt de discos redundants, protegeix contra la pèrdua de dades i proporciona la recuperació de les dades en temps real.
Pèrdua d'integritat en la informació	• Ús de programes de revisió mèdica de l'equip, SiSoft Sandra 2000, TuneUp... • Mitjançant la forma digital en ela envio d'informació a través de missatges enviats per la xarxa. • Ús de la instrucció del SOTA Windows, sfc (System file checker).
Entrada de virus	• Ús d'antivirus, que eviti que s'infectin els equips amb programes malintencionats.
Atacs des de la xarxa	• *Firewall*, autoritzat i auditant les connexions permeses. • Programes de monitoratge. • Servidors proxys, autoritzant i auditant les connexions permeses.
Modificacions no autoritzades	• Ús de contrasenyes que no permetin l'accés a la informació. • Ús de llistes de control d'accés. • Xifrar documents.

4. Diferències entre Seguretat Física i Lògica en els sistemes d'informació

Mentre que la **Seguretat Lògica** protegeix el programari informàtic mitjançant la implementació d'identificacions d'usuari, contrasenyes, autenticació, biometria i targetes intel·ligents, **la Seguretat Física** evita i descoratja als atacants a ingressar a un edifici instal·lant **tanques, alarmes, càmeres, guàrdies de seguretat i gossos, controls d'accés electrònic, detecció d'intrusos i controls d'accés d'administració**.

La diferència entre la Seguretat Lògica i la Seguretat Física és que la **Seguretat Lògica protegeix l'accés als sistemes informàtics** i la **Seguretat Física protegeix el lloc** i tot el que es troba dins d'aquest.

El terme **Seguretat lògica** s'utilitza de forma col·loquial per a referir-se a **mesures electròniques** com són els permisos dins del sistema operatiu o les regles d'accés en les capes de la xarxa (*firewalls*, enrutadors i commutadors). La **Seguretat Física** s'usa tradicionalment per a **descriure portes d'entrada controlades, videovigilància i altres mesures metafísiques**.

La superposició entre els dos és cada vegada major, ja que **els sistemes que proporcionen Seguretat Lògica tenen algunes mesures també de Seguretat Física**.

https://freepik.es

5. Per què és tant important la Seguretat Lògica a les organitzacions?

Malgrat la preocupació pels atacs de ciberseguretat i els desastres naturals que cada vegada es produeixen amb major freqüència, la veritat és que la majoria del temps d'inactivitat del servidor és causat per un error humà. La Seguretat Lògica no sols redueix la possibilitat d'errors humans en limitar l'accés, sinó que també fa que sigui més fàcil rastrejar els errors i diagnosticar els problemes quan aquests succeeixen.

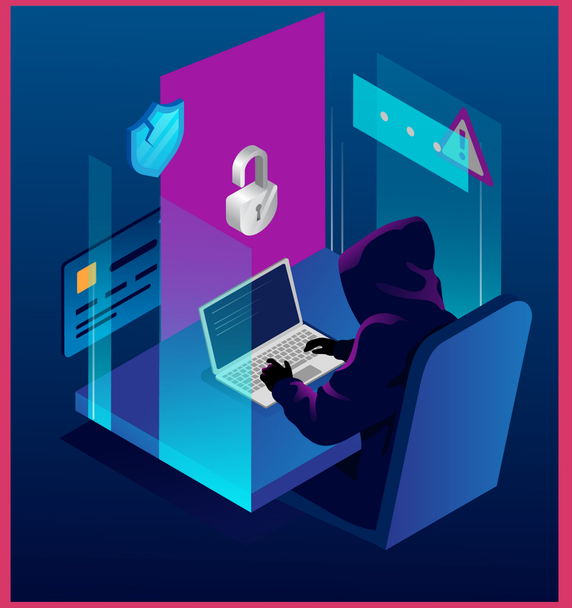
Els ciberdelinqüents poden penetrar en una xarxa de diverses maneres, des d'intents de pirateria per força bruta fins a estratègies de *phishing* perfectament elaborades a aquest efecte. La Seguretat Lògica proporciona una capa addicional de defensa contra aquestes intrusions.

No obstant això, la Seguretat Lògica pot no oferir protecció contra totes les formes d'atacs cibernètics. És cert que pot reduir en gran manera el risc d'accessos no autoritzats i permetre als experts en Seguretat de la Informació rastrejar intrusions de manera més efectiva quan aquestes ocorren, però no garanteixen una protecció al 100%.

Treballar i emmagatzemar la informació al núvol (pràctica cada vegada més habitual en les organitzacions) ha fet possible que les persones accedeixin al núvol públic o privat del seu lloc de treball de manera remota amb gairebé qualsevol dispositiu que pugui connectar-se en línia. Això ha creat problemes per a moltes organitzacions, ja que qualsevol d'aquests dispositius, des de portàtils fins a telèfons intel·ligents, podrien representar una amenaça per a la seguretat.

Per exemple, el Codi maliciós incrustat en un sistema operatiu d'un portàtil podria infectar fàcilment una xarxa segura en el moment en què es connecta el dispositiu. En aquest cas, es podrien establir protocols lògics d'accés de seguretat a l'hora d'administrar els dispositius professionals o personals que són usats pels empleats. D'aquesta manera, es permet a les empreses poder bloquejar els dispositius que s'extraviïn i restringint l'ús de dispositius personals per a un ús estrictament professional.

Per tant, les mesures de Seguretat Lògiques formen un component important en les operacions de qualsevol centre de dades. Encara que cap mesura de seguretat és completament invulnerable, les organitzacions poden combinar la Seguretat Lògica amb les seves estratègies físiques i de Ciberseguretat per tal d'oferir la millor protecció possible.



https://stock.adobe.com

6. Altres dades curioses: Millors pràctiques de Seguretat Física i Lògica en la seva CPD

https://freepik.es

Millors pràctiques de seguretat lògica pel vostre CPD:

Per tal d'evitar que els cibercriminals puguin accedir al vostre CPD (Centre de Processament de Dades), es necessita una estratègia de seguretat enfocada a la prevenció i detecció d'incidents, per la qual cosa recomanem tenir en compte les següents accions:

- **Gestió de riscos.**
- **Segmentació de xarxes i equips crítics.**
- **Tallafocs físics i virtuals:** pel cas que es tingui una infraestructura híbrida o al núvol.
- **IPS o sistemes de prevenció d'intrusos.**
- **Adequació de permisos.**
- **Controls integrals de seguretat.**
- **Gestió d'accessos privilegiats.**
- **Solucions de prevenció de pèrdua de dades.**
- **Pla de recuperació abans desastres.**
- **SIEM (correlacionador d'esdeveniments).**
- **Pla de detecció i resposta davant incidents de seguretat.**

Millors pràctiques de seguretat física pel vostre CPD:

Per tal d'evitar que el vostre personal no autoritzat pugui accedir al seu CPD (Centre de Processament de Dades), recomanem tenir en compte les següents accions:

- **Control d'accés:** Validar l'entrada del personal al CPD, mitjançant targetes personals o sistemes biomètrics.
- **Vigilància 24/7:** Zones exteriors ben vigilades pel personal de seguretat.
- **Climatització dels servidors:** Monitoratge periòdic de la temperatura i la seva climatització.
- **Sistemes de videovigilància/alarma:** Suport amb càmares i alarmes per a detectar intrusions l'abans possible.
- **Protecció contra incendis:** Cuidar bé el CPD de l'exposició al foc.