Seguretat física i lògica d’una nau industrial

La combinació de seguretat física i seguretat lògica és essencial per garantir la continuïtat operativa i la protecció tant dels béns físics com de la informació. En aquesta pràctica treballarem la seguretat física i lògica que cal complir.

Seguretat física

La seguretat física se centra en protegir els béns materials i les persones dins de la nau industrial.

Mesures de Seguretat Física:

- Control d’accés: Implementació de sistemes de control d’accés, com targetes d’identificació, lectors de targetes, claus biomètriques o codis de seguretat per restringir l’entrada a zones sensibles (com magatzems, oficines o laboratoris).

- Tanques i portes de seguretat: Instal·lar tanques perimetrals al voltant de la nau industrial i assegurar-se que totes les entrades i sortides estiguin ben protegides amb portes reforçades i panys electrònics.

- Videovigilància: Utilització de càmeres de seguretat (CCTV) per monitoritzar tant l’interior com l’exterior de les instal·lacions. Això pot servir per dissuadir robatoris, detectar intrusions i recopilar proves en cas d'incidents. Emmagatzematge de les gravacions.

- Il·luminació: Una il·luminació adequada a l’exterior de la nau industrial redueix les oportunitats d’intrusió durant la nit. Amb sensor de moviment per eficàcia energètica.

- Sistemes d’alarma amb sensors de moviment: Instal·lació de sistemes d'alarma contra robatoris o intrusions que notifiquen automàticament les autoritats o el personal de seguretat.

- Seguretat privada: Disposar de personal de seguretat per realitzar rondes de vigilància o monitoritzar les càmeres i sistemes d'alarma en temps real.

- Dispositius d’emergència: Sortides d'emergència i senyals clars per a una evacuació segura en cas d'incident.

- Protecció envers les condicions ambientals: Protecció contra inundacions mitjançant sistemes de drenatge i sensors, aïllament tèrmic i estructures reforçades per resistir vents forts o terratrèmols.

- Sistemes de control de temperatura i humitat per preservar materials sensibles, així com filtres per protegir la nau de contaminants externs. Els sistemes de ventilació a més de tenir la funció de refrigerar també són importants per evitar l’acumulació de pols i d’altres agents contaminants.
  Els elements que formen un sistema d'aire condicionat són l’evaporador, que s’instal·la a l’interior i el condensador, que aspirar l'aire de l'exterior usant compressor i ventilador.
  La temperatura òptima és entre 18ºC i 24ºC. La humitat relativa òptima és entre 45% i 55%.

- Protecció contra incendis: Sistemes de detecció i extinció d'incendis (extintors, detectors de fum, ruixadors automàtics) han d'estar implementats i regularment verificats. La distància entre extintors ha de ser com a màxim de 15 metres.

Classe	Tipus de foc	Elements de combustió	Mètodes d'extinció
A	Comú	Fusta, paper...	Aigua, escuma
B	Líquid	Petroli, carbó...	CO_2, escuma
C	Elèctric	Cables, material elèctric...	CO_2, pólvora seca
D	Metalls inflamables	Magnesi, sodi, potassi...	Pólvora seca

- Sistema d'Alimentació Ininterrompuda (SAI): Dispositiu que proporciona energia temporal en cas de tall de llum per protegir equips electrònics, pot ser útil per mantenir el servei dels servidors. Per calcular el nombre de SAIs necessaris tingues en compte el següent:

Característiques dels SAIs:

- **Potència de subministrament del SAI (P):** expressada en watts (W), ha de ser com a mínim un 20% superior a la suma de les potències de consum dels dispositius connectats a ell.
- **Potència aparent (S):** mesura en volt-amperes (VA), és una altra manera de representar la potència de subministrament sense comptar amb el factor de potència.
- **Temps d'autonomia:** és una estimació, ja que dependrà dels dispositius connectats al SAI i de la seva potència, del temps del qual es disposa per a treballar sense corrent extern.
- **Protecció de línia telefònica:** molts SAIs ofereixen dos ports RJ-11 (un d'entrada i un de sortida) per a regular la tensió que circula per la línia telefònica. Una pujada o una caiguda de tensió per aquesta línia podria deixar-nos sense *encaminador* o mòdem ADSL.

Seguretat lògica

La seguretat lògica protegeix la informació digital i els sistemes informàtics dins la nau industrial.

Mesures de Seguretat Lògica:

- Control d'accés: Integrat a les mesures de seguretat físiques per la gestió d'identitats i autenticació del sistema. Permet mantenir registre d'entrades i sortides.

- Tallafocs (Firewall): Implementació de tallafocs per protegir la xarxa interna de la nau industrial davant d'atacs cibernètics o accessos no autoritzats des d'internet.

- Antivirus i antimalware: Els sistemes informàtics han d'estar protegits amb solucions antivirus actualitzades per detectar i eliminar programari maliciós que pugui infectar la xarxa.

- Xarxes segmentades: Creació de xarxes separades per a diferents funcions (per exemple, una per a l'administració i una altra per als sistemes de producció), de manera que una intrusió en una part no afecti altres àrees crítiques. Implementació de VLANs.

- Còpies de seguretat (backups): Mantenir còpies de seguretat regulars de les dades crítiques, ja sigui localment o al núvol, per prevenir pèrdues d'informació en cas d'atacs o errors.

- Xifratge de dades: Protegir la informació sensible amb tècniques de xifratge, tant a nivell d'emmagatzematge com en les comunicacions (xifratge de correus electrònics, de comunicacions dins de la xarxa). Assegura't que el xifratge compleixi amb les normatives i estàndards de seguretat vigents.

- Control d'accés a sistemes: L'ús de contrasenyes fortes, l'autenticació de dos factors (2FA) i l'assignació de permisos d'accés adequats segons el rol dels empleats per evitar accessos indeguts.

- Monitorització de xarxa: Implementar eines per monitoritzar l'activitat de la xarxa, amb l'objectiu de detectar i respondre ràpidament a qualsevol anomalia o atac cibernètic.

- Polítiques de seguretat: Establir polítiques d'ús dels sistemes informàtics i formació per als empleats sobre les bones pràctiques de seguretat (per exemple, no compartir contrasenyes, evitar l'ús de dispositius USB no segurs, etc.).

- Actualització i Manteniment: Mantingues els sistemes actualitzats amb els darrers pegats de seguretat i actualitza les polítiques i procediments segons sigui necessari per afrontar nous riscos.

ACTIVITATS

1. **L’empresa de nova creació SL S.L. necessita un pla de seguretat per planificar les instal·lacions.**

Aquestes són les diferents zones que requerirà l’empresa amb els elements fonamentals que l’integren:

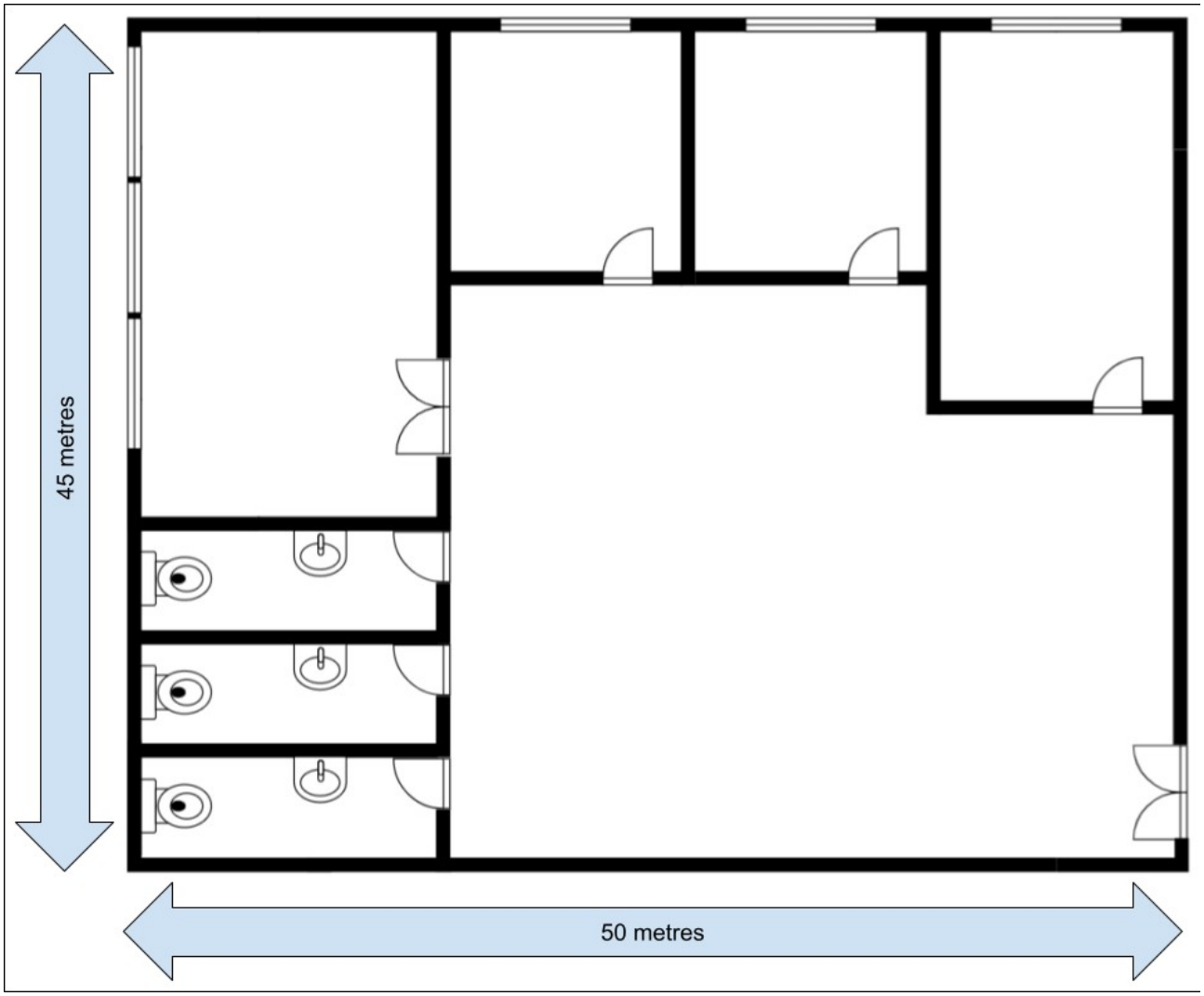
Sala de servidors	Taller mecànic
1 armari rack de servidors	2 taladradores
1 patch panel	1 fresadora
1 switch	1 torn manual
1 servidor web	1 ordinador
1 servidor de dades	1 punt d’accés sense fils
	1 impressora

Departament de vendes i màrqueting	Direcció
4 ordinadors	2 ordinadors
1 impressora	1 impressora/escàner
1 escàner	

Pots agrupar-les o dividir-les creant-ne de noves segons el teu criteri i les necessitats que detectis.

a) Plànol físic de l'empresa

Aquest és el plànol de la nau que l'empresa ha comprat, si no et sembla adequat fes una proposta de les obres que si haurien de realitzar.
La nau es troba en una zona boscosa, prop d'un riu no canalitzat.



Per cada zona, indica el següent al plànol:

- Nom de la zona.
- Delimitació clara.
- Distribució: Posa icones per indicar els elements que conté.
- Àrea: *Àrea (m^2)= base * alçada*.

Afegeix una llegenda al costat del plànol per indicar què és cada icona inclosa al plànol.

b) Anàlisi del risc

Avalua els riscos físics i lògics a que estan sotmesos els actius informàtics de l'organització.

Emplena aquesta taula identificant les vulnerabilitats potencials, els riscos associats, l'impacte i avalua el risc com a baix (0,1), mitjà (0,3) o alt (0,5). Cerca dades estadístiques per decidir aquests valors.

Per avaluar si el risc justifica la inversió econòmica calcula l'EMV (Expected Monetary Value):
EMV = Risc * Impacte
Si l'EMV és superior a la inversió a realitzar per reduir el risc, aquesta inversió és imprescindible.

Agrupa'ls en riscos físics i lògics.

Amenaça	Vulnerabilitat	Risc (%)	Impacte (€)	EMV (€)
...	...	...	...	...

c) Plànol de seguretat física i climatització

Investiga i proposa de manera justificada possibles mesures de seguretat física (activa o passiva) que siguin proporcionades i que permetin rebaixar el risc al que estan sotmesos els equips informàtics d'aquesta empresa.

Al plànol proporcionat per l'empresa afegeix-hi els elements de seguretat física per tal de protegir a les persones i els béns de l'empresa.

Afegeix a cada zona de la nau la temperatura i humitat recomanada.

Dibuixar els evaporadors i els condensadors necessaris. Especifica clarament en el plànol la posició de l'evaporador i del condensador.

Per a dibuixar els elements de seguretat utilitzar símbols representatius per a cada element i afegir-los a la llegenda.

d) Pla de seguretat lògica

Indica les mesures de seguretat lògica: Desenvolupa polítiques clares que descriguin com es protegiran les dades i els sistemes, incloent l'ús acceptable de recursos, control d'accés, gestió de contrasenyes, etc.

Resposta a Incidents: Desenvolupa un pla de resposta a incidents per gestionar i mitigar les repercussions d'un incident de seguretat, incloent la comunicació amb les parts afectades, la restauració dels serveis i la recuperació de dades.

e) Pressupost

Realitzar un pressupost aproximat del pla de seguretat físic i lògic, separa'ls adequadament. Inclou en el pressupost els elements de seguretat que has descrit anteriorment. Indica el cost total.

Descripció element, imatge i enllaç	Quantitat	Preu/unitat	Total
...	...	...	...

f) CPD

Què és un CPD?

Anomena cinc elements informàtics que es poden trobar en un CPD i quines amenaces els poden afectar. Digues algunes mesures de seguretat per protegir-lo.

Indica quina és la temperatura i la humitat relativa en un CPD.

Busca informació sobre quin tipus de extintor és més recomanable per a un CPD.

BIBLIOGRAFIA I WEBGRAFIA

«c3comunicaciones». https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/
Pou, Joan.
«TutorialsPoint». https://www.tutorialspoint.com/what-is-the-difference-between-physical-security-and-logical-security-in-information-security
«Visual Paradigm Online». https://online.visual-paradigm.com/diagrams/templates/floor-plan/work-office/office-floor-plan-with-conference-room/