

Activitat 2 Clínica Dental

Albert Molinas

Pol de la Viuda

Contenido

Llistat d'arxius	3
Dades	3
Maquinari	3
Programari.....	3
Xarxes	3
Personal.....	3
Instal·lacions	3
Seguretat física i lògica	3
Físiques.....	3
Lògiques.....	3
Anàlisi de vulnerabilitats	3
Debilitats	3
CIA	4
Confidencialitat	4
Integritat	4
Disponibilitat	4
Serveis i mecanismes de seguretat	4
Confidencialitat	4
Autenticació	4
Disponibilitat	4
Mecanismes	4
Preventius	4
Detectors	4
Correctors	4
Polítiques de seguretat i pla de contingències	4
Auditoria informàtica.....	5

Llistat d'arxius

Dades: Historials mèdics, dades personals de pacients, agenda digital, facturació i contrasenyes.

Maquinari: Els ordinadors de les consultes i la recepció, el servidor, el router i la impressora.

Programari: Programes de gestió clínica, ofimàtica, antivirus, sistema operatiu, correu.

Xarxes: La xarxa interna, internet, router, possible WiFi per a empleats/pacients.

Personal: Odontòleg, especialista, auxiliars, administratiu i neteja.

Instal·lacions: Consultes, recepció, despatx del servidor i magatzem.

Seguretat física i lògica

Tenen el bàsic, el servidor és en un despatx separat i els ordinadors no estan a l'abast de tothom.

Però es podrien millorar diverses coses:

Físiques: posar un pany més segur al despatx del servidor, càmeres i còpies de seguretat fora de la clínica.

Lògiques: contrasenyes més segures i diferents per a cada usuari i xifrat de dades mèdiques.

Anàlisi de vulnerabilitats

Debilitats:

- El servidor no està del tot protegit físicament
- Pot ser que comparteixin contrasenyes entre diversos treballadors

- Els pacients i el personal utilitzen la mateixa xarxa
- No sembla que tinguin còpies de seguretat fora
- Falta formació en seguretat per al personal

CIA:

Confidencialitat: algú podria veure dades de pacients

Integritat: es podrien modificar o esborrar dades sense control

Disponibilitat: si cau el servidor, es queden sense accés a tot

Serveis i mecanismes de seguretat

El que més necessiten és:

Confidencialitat: xifrar la informació

Autenticació: que cada treballador tingui el seu usuari

Disponibilitat: còpies de seguretat i un pla B si el servidor falla

Mecanismes:

Preventius: formació, contrasenyes segures, xifrat.

Detectors: control d'accessos i alertes.

Correctors: còpies de seguretat i recuperació ràpida.

Polítiques de seguretat i pla de contingències

Sí o sí haurien de tenir una política de seguretat, perquè treballen amb dades personals i mèdiques que estan protegides per llei. Això els serviria per marcar normes clares (per exemple, com usar contrasenyes o qui pot accedir a què).

També necessiten un pla de contingències, perquè si els falla el servidor, si els hackegen o fins i tot si es talla la llum, no poden deixar d'atendre els pacients.

Auditoria informàtica

Recomanem que facin una auditoria externa, ja que així un equip expert pot revisar si compleixen la llei, buscar errors que ells no veuen i aconsellar millores adaptades a la mida de la clínica