Quan la tecnologia entra a l'aula, quin és el paper dels síndics de greuges?

La visió tecnològica

Índex

1. Introducció

Amb que ens trobem?

- He enviat una presentació al Langblog i no ha arribat
- M'han esborrat un arxiu que havia penjat
- M'han plagiat una PAC que havia penjat en una xarxa social
- ...

Crime Scene 1

Crime Scene 2

Que és pot fer?

Però la imaginació no té límits

I els mecanismes de control tampoc 1/2

I els mecanismes de control tampoc 2/2

El projecte TeSLA

I com pot ajudar la tecnologia?

2. Seguretat de la informació

Propietats vinculades a la informació

DISPONIBILITAT

Assegurar que els usuaris autoritzats tenen accés quan ho requereixin a la informació i als seus actius associats.

CONFIDENCIALITAT

Assegurar que la informació és accessible només per aquells autoritzats a tenir accés.

INTEGRITAT

Garantir l'exactitud i completitud de la informació i els mètodes del seu processament

La gestió eficaç de la **Seguretat de la Informació** permet a l'organització preservar-les.

Model de millora contínua

Definir política de seguretat
Establir abast del SGSI
Realitzar anàlisi de riscos
Seleccionar els controls

PLAN

Implantar pla de gestió de riscos
Implantar el SGSI
Implantar els controls

DO

ISO IEC 27002	
A.5 Política de Seguretat d'Informació A.6 Organització de la Seguretat de la informació A.7 Seguretat en els RRHH A.8 Gestió d'Actius A.9 Control d'Accessos A.10 Criptografia A.11 Seguretat Física i ambiental A.12 Seguretat en les operacions	A.13 Seguretat en les comunicacions A.14 Adquisició, desenvolupament i manteniment de sistemes A.15 Relació amb proveïdors A.16 Gestió d'incidents de seguretat A.17 Aspectes de Seguretat de la informació dins de continuïtat de negoci A.18 Conformitat

ACT

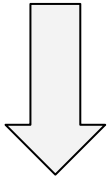
Adoptar les accions correctivas
Adoptar les accions preventives

CHECK

Revisar internament el SGSI
Realitzar auditorias internes del SGSI
Indicadors i Mètriques
Revisió per Direcció

Anàlisi i Gestió de riscos - Implantació de controls

Procesos de Negoci / Serveis de TI



Actius de SI

- Sistemas d'informació
- Software
- Hardware
- Telecomunicacions
- Persones

Anàlisi i gestió de riscos

R=F(X1,X2,X3,... Xn)

- Integritat (X1)
- Confidencialitat (X2)
- Disponibilitat (X3)
- Amenaces (X4)
- Vulnerabilitats (X5)
- Impacte Econòmic (X6)
- Xn

Risc residual

Actiu1 → R'1
Actiu2 → R'2

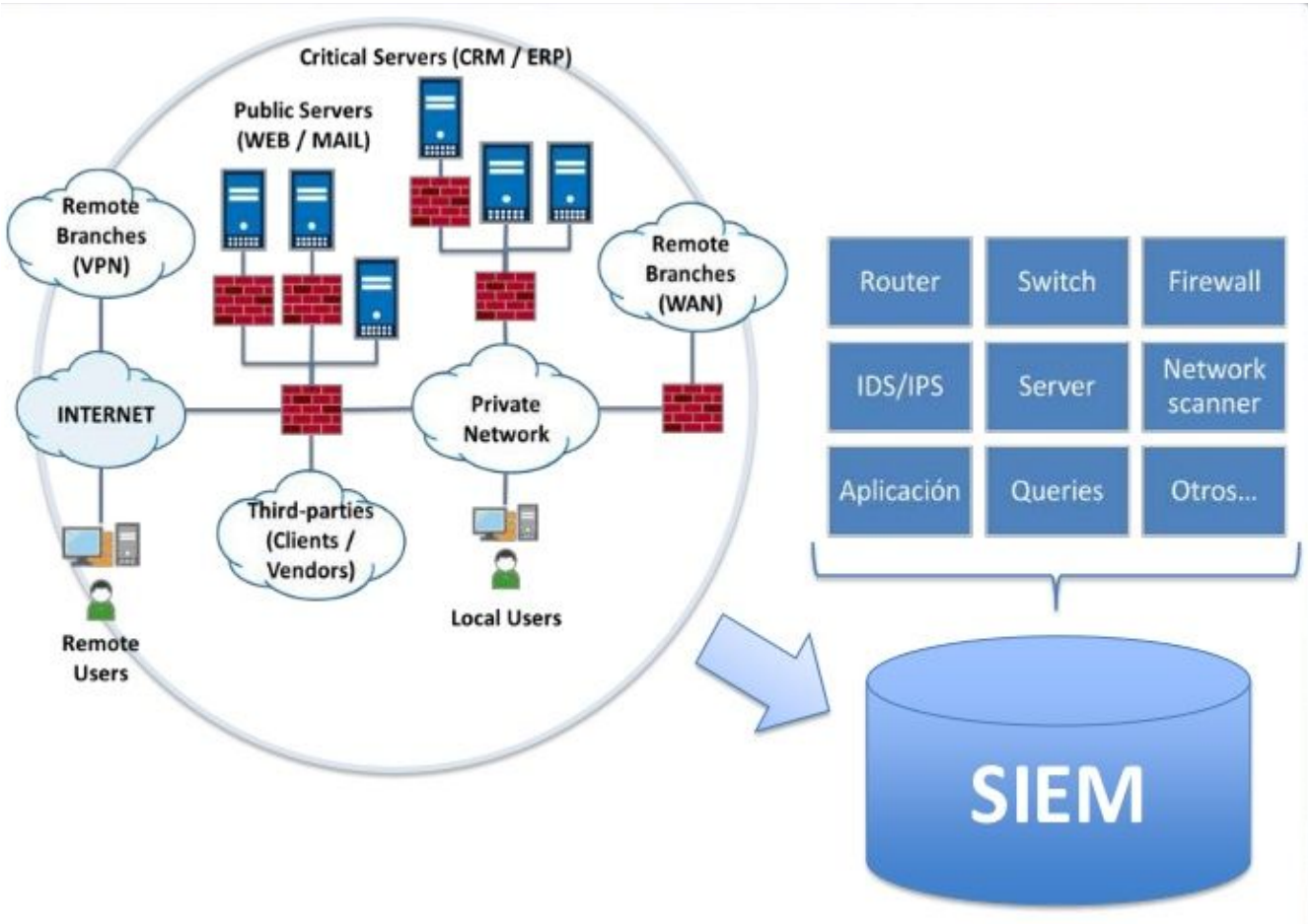
Aplicant ISO/IEC 27002

3. Gestió d'evidències

Qué és una evidència electrònica?

- Són dades emmagatzemades en suport digital
- Han estat recol·lectades seguint mètodes tècnics especialitzats auditables, reproduïbles i defensables
- Els processos de recol·lecció han de contemplar la: identificació, recol·lecció, adquisició, conservació i preservació.
- S'ha d'assegurar que l''evidència no ha pogut ser modificada
- Tenen una finalitat de prova fefaent

security information and event management (SIEM)



Característiques d'un SIEM

- **Integritat**: facilitant la detecció de canvis en l'evidència.
- **Preservació**: aportant mecanismes que permeten independitzar-se de la caducitat de certificats o d'algorismes criptogràfics.
- **Verificabilitat**: oferint un mètode per verificar l'autenticitat de l'evidència generada.
- **Trazabilidad de l'origen**: garantir que l'evidència es pot associar al seu autor i detectar suplantacions.
- **Datat**: associant de forma segura l'evidència a un moment temporal.
- **Seqüencialitat**: aplicant un ordre i mecanisme comprovació de l'encadenament de diferents esdeveniments de tal forma que pugui detectar-se la inserció o l'esborrat d'un esdeveniment entre dos ja existents.
- **Custòdia**: facilitant un arxiu segur, que garanteix la disponibilitat íntegra de l'evidència juntament amb un control d'accés.
- **Confidencialitat**: La informació pot ser xifrada en trànsit o en emmagatzematge mitjançant un algorisme de xifrat amb clau simètrica o pública.

4. Privacitat en el disseny

Privacitat en el disseny

És una aproximació a la protecció de la privacitat tenint-la en compte des de l'inici en:

- El disseny de les tecnologies
- Les pràctiques de negoci
- Les infraestructures físiques

Es basa en 7 principis i es va desenvolupar inicialment per la Dra. Ann Cavoukian (Ontario's Information and Privacy Commissioner) als 90s,

https://privacybydesign.ca

1.Proactiu no reactiu; preventiu no correctiu

La privadesa des del disseny sol caracteritzar-se per prendre mesures proactives en lloc de reactives. S'anticipa i prevé la pèrdua de privadesa de la informació abans que aquesta succeeixi. Si això ha ocorregut, es troba fora de l'abast d'aquest concepte.

2.La privadesa com a configuració per defecte

Oferir el màxim grau de privadesa per assegurar que les dades personals estan protegits automàticament en qualsevol sistema informàtic o dins de les bones pràctiques. Sense necessitat d'actuació per part del client o proveïdor, la protecció de la seva informació i la seva privadesa es manté intacta, ja que això està integrat en el sistema per defecte.

3.La privadesa embeguda en el disseny

La protecció de la informació està incorporada en la infraestructura de la tecnologia i en els processos de l'organització. No és considera com un afegit, sinó com un component essencial del nucli i com a part integral del sistema, sense disminuir la funcionalitat.

4.Funcionalitat completa - Positiu-Suma, no de suma zero

Amb aquest principi es pretén donar cabuda a tots els interessos i els objectius d'una forma de suma positiva win-win entre diferents interessos dels departaments respecte a la gestió de la informació. A més, així s'evitan falses divisions entre privadesa i seguretat.

5.Seguretat extrem-a-extrem

Protecció completa del cicle de vida: des del moment de la seva recol·lecció, la protecció s'estén a través de tot el cicle de vida de les dades involucrades. D'aquesta manera, totes les dades es conserven i destrueixen de forma segura, assegurant la gestió del cicle de vida segur de la informació des del principi fins al final.

6.Visibilitat i transparència - Mantenir-ho obert

Garantir a tots els interessats que, siguin quines siguin les bones pràctiques o la tecnologia utilitzades, funcionaran d'acord amb els compromisos i els objectius establerts, i que estaran subjectes a una verificació independent. D'aquesta forma els components i operacions romanen visibles i transparents, als usuaris i proveïdors per igual. Recorda: Confiar però verificar.

7.El respecte a la privadesa de l'usuari - Disseny centrat en l'usuari

Per sobre de tot, és obligació d'arquitectes i operadors del sistema mantenir els interessos de les persones, oferint com a valors predeterminats de privadesa mesures fortes, amb avisos apropiats, i potenciant opcions fàcils d'utilitzar i amb un disseny centrat en l'usuari.

5. Conclusions

Algunes idees

- La importància creixent de la tecnologia a l'aula
- Els aspectes de seguretat són crítics per garantir els drets de la comunitat universitària
- Conscienciació de totes les persones que intervenen
- Aliniament entre aspectes legals i tecnològics
- La gobernança de la seguretat és un aspecte primordial
- La privacitat des del disseny com a principi


UOC
Universitat Oberta
de Catalunya