



Centre
de Telecomunicacions
i Tecnologies
de la Informació

Aspectes organitzatius lligats a la Seguretat de la Informació

NcN 2010

Índex

- Estructura Organitzativa de Seguretat: Per què?
 - Què ens ha ensenyat l'experiència?.
 - D'on sorgeix la idea? És nova?.

- Construint una estructura organitzativa de seguretat.
 - Quina és la millor estructura?
 - Algunes reflexions i consells....
 - Criteris en l'elecció dels components del CSI.

Estructura Organitzativa de Seguretat: Per què?

Què ens ha ensenyat l'experiència?

- Per garantir la seguretat, la tecnologia és necessària.

- Sense determinats dispositius tecnològics.....

Firewalls, IDS/IPS, Sistemes anti-virus, Antispam, Eines de monitorització, Eines de detecció de vulnerabilitats, Correlació de logs (de sistema, d'aplicació).....
....però NO és suficient.

-es fa difícil poder garantir la seguretat.
- La tecnologia permet l'aplicació de moltes mesures i controls de seguretat de forma automatitzada.
 - És més, molts controls no es podrien aplicar sense mitjans tecnològics.

Estructura Organitzativa de Seguretat: Per què?

Què ens ha ensenyat l'experiència?

□ Llavors, per què no es suficient?

- L'aplicació d'alguns controls de seguretat acostumen a ser "poc populars" entre la major part dels usuaris:

✓ Inhabilitació de ports USB per a l'extracció d'informació.

✓ Filtrat d'URL's.

✓ Impossibilitat d'instal·lar programari per part de l'usuari de transaccions digitals per delictes de seguretat (falsificació de transaccions, etc.)

✓ Utilització de certificats

✓ Bloqueig de treball remot i cancel·lació de sessió.

✓ Impossibilitat d'instal·lar equips de sensors a la xarxa corporativa.

✓ Longitud mínima de les contrasenyes o Canvis periòdics de les contrasenyes

✓

Per tant, no es tracta d'un problema tecnològic → Cal gestionar del canvi.

- Quan aquestes iniciatives són liderades per les àrees tècniques, es qüestiona la seva necessarietat, dificultant la implantació.
- En canvi, si aquestes iniciatives tenen el suport de la Direcció (per exemple, estan recollides a la Política de Seguretat).....deixen de ser qüestionades.

Estructura Organitzativa de Seguretat: Per què?

Què ens ha ensenyat l'experiència?

- Llavors, per què no és suficient?
 - Determinades decisions estratègiques de seguretat s'han de prendre a un nivell directiu adequat.
 - Per exemple, aquelles que requereixen inversió i, per tant, l'autorització de la dotació pressupostària adient.

Garantir l'alta disponibilitat d'un sistema

✓ Redundància d'equips

✓ Balanceig de càrrega

✓ Escalabilitat de recursos

✓ Copia de seguretat

Les iniciatives de seguretat necessiten el suport (i recursos) de la Direcció

- Les decisions en seguretat han de tenir present el principi de proporcionalitat i l'impacte en el risc global.

Estructura Organitzativa de Seguretat: Per què?

D'on sorgeix la idea? És nova?

- Existeixen diversos estàndards internacionals que estableixen la importància de disposar d'una estructura organitzativa de seguretat:
 - ISO 27002, publicada l'any '00 com ISO 17799: Domini 6, Organització de la Seguretat de la informació.
 - COBIT, 3rd Edition '00:
 - Domini PO4: Definir els processos, organització i relació IT.
 - Domini PO6: Comunicar els objectius de gestió i direcció).
 - NIST
 - SP 800-12 ('95): An Introduction to Computer Security.
 - SP 800-55 ('08): Security Metrics Guide for Information Technology Systems, Cap. 2.
 - ...
- Existeix també legislació específica, com ara l'Esquema Nacional de Seguretat, on es fa referència als aspectes organitzatius lligats a la seguretat.
 - Annex II, punt 3: Marc organitzatiu.

Per tant, aquesta idea no és nova

Estructura Organitzativa de Seguretat: Per què?

D'on sorgeix la idea? És nova?

- Disposar d'una estructura organitzativa permet afrontar tot el seguit d'accions no tècniques que normalment queden "en terreny de ningú" o, simplement, no es duen a terme.

✓ Politiques i normes de seguretat per a l'ús de les TIC.

✓ Accions de formació, difusió i conscienciació.

✓ Compliment normatiu.

✓ Inclusió de

la informació dels controls organitzatius per garantir la CID de

✓ Documentació dels controls organitzatius de la informació.

✓

El 42% (aprox.) dels controls recollits a la norma ISO 27002 són controls organitzatius (no tècnics)

Construint una Estructura Organitzativa

Quina és la millor estructura de seguretat?

- Aquella que funciona en una organització.
 - Cada organització té les seves particularitats.....
 - El que funciona en una organització, no té per què funcionar en una altra.
 -no hi ha “receptes màgiques” que garanteixin l’èxit.
 - Tot i això es recomana tenir presents alguns consells que poden ajudar a establir la millor estructura organitzativa.

Construint una Estructura Organitzativa de Seguretat

Algunes reflexions i consells....

- ❑ El suport de la **Direcció** en les iniciatives de seguretat és un factor crític, com s'ha vist anteriorment.
- ❑ La seguretat ha d'estar alineada amb els objectius de **negoci**, de fet, hauria d'ajudar a que s'aconsegueixin els objectius de negoci
- ❑ Les **àrees de negoci** amb **informació més crítica** són les que tenen majors requeriments de seguretat.
- ❑ El punt focal en seguretat de la informació hauria de ser el **Responsable de Seguretat de la Informació**.
- ❑ Les persones que formin part de l'estructura organitzativa de seguretat haurien de tenir:
 - Coneixement ampli de l'organització (visió transversal).
 - Capacitat de presa de decisió.
- ❑ L'aportació de les **TIC** és un element clau per al desplegament de les mesures i controls de seguretat.
- ❑ Els requeriments **legals** acostumen a tenir impacte en la seguretat (p.ex.: LOPD, LSSI).
- ❑ La gestió del canvi en la implantació de mesures de seguretat (conscienciació, difusió, formació, etc.) l'hauria de liderar l'àrea d'**organització**.

Construint una Estructura Organitzativa de Seguretat

Algunes reflexions i consells....

- El suport de la **Direcció** en les iniciatives de seguretat és un factor crític, com s'ha vist anteriorment.
- La seguretat ha d'estar alineada amb els objectius de **negoci**, de fet, hauria d'ajudar a que s'aconsegueixin els objectius de negoci.
- Les **àrees de negoci** amb **informació més crítica** són les que tenen majors requeriments de seguretat.
- El punt focal en seguretat de la informació ha de ser el **Responsable de Seguretat** de la Informació.
- Les persones que formen part de l'estructura organitzativa de seguretat haurien de tenir:
 - Coneixement aprofundit en seguretat (visió transversal).
 - Capacitat per prendre decisions.
- L'aportació de les **TIC** és un element clau per al desplegament de les mesures i controls de seguretat.
- Els requeriments **legals** acostumen a tenir impacte en la seguretat (p.ex.: LOPD, LSSI).
- La gestió del canvi en la implantació de mesures de seguretat (conscienciació, difusió, formació, etc.) l'hauria de liderar l'àrea **organització**.

Sembla que aquestes figures haurien d'estar representades en l'estructura organitzativa

Construint una Estructura Organitzativa de Seguretat

Alguns consells....

- Els estàndards internacionals (i l'experiència en la implantació de sistemes de gestió) recomanen una estructura jeràrquica diferenciant, almenys, 3 nivells organitzatius:

Direcció

- **Nivell *Estratègic*.**

- Presa de decisions: Aprovar les principals iniciatives per a incrementar la seguretat.
- Seguiment d'alt nivell: Vetllar per la bona gestió i adopció de les mesures apropiades.

CSI

- **Nivell *Tàctic*.**

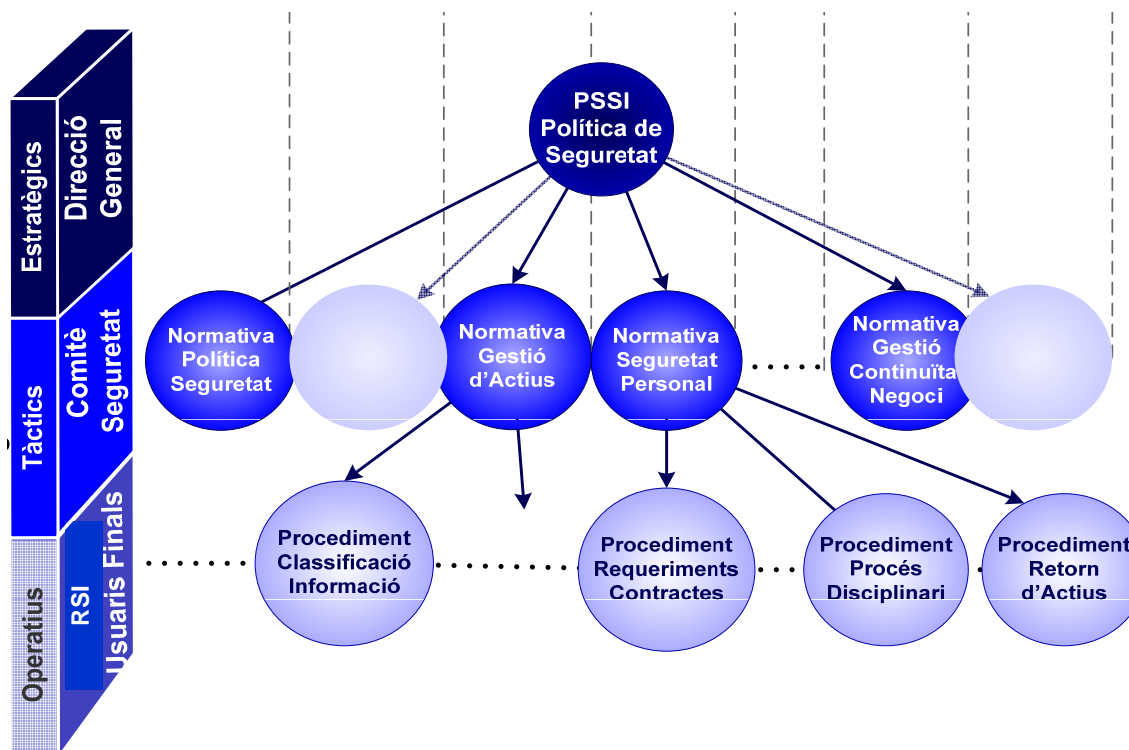
- Liderar la implantació de les directrius i actuacions en matèria de seguretat de la informació.
- Presentar a aprovació al nivell estratègic les iniciatives, supervisar-les i fer-ne el seguiment.

RSI

- **Nivell *Operatiu*.**

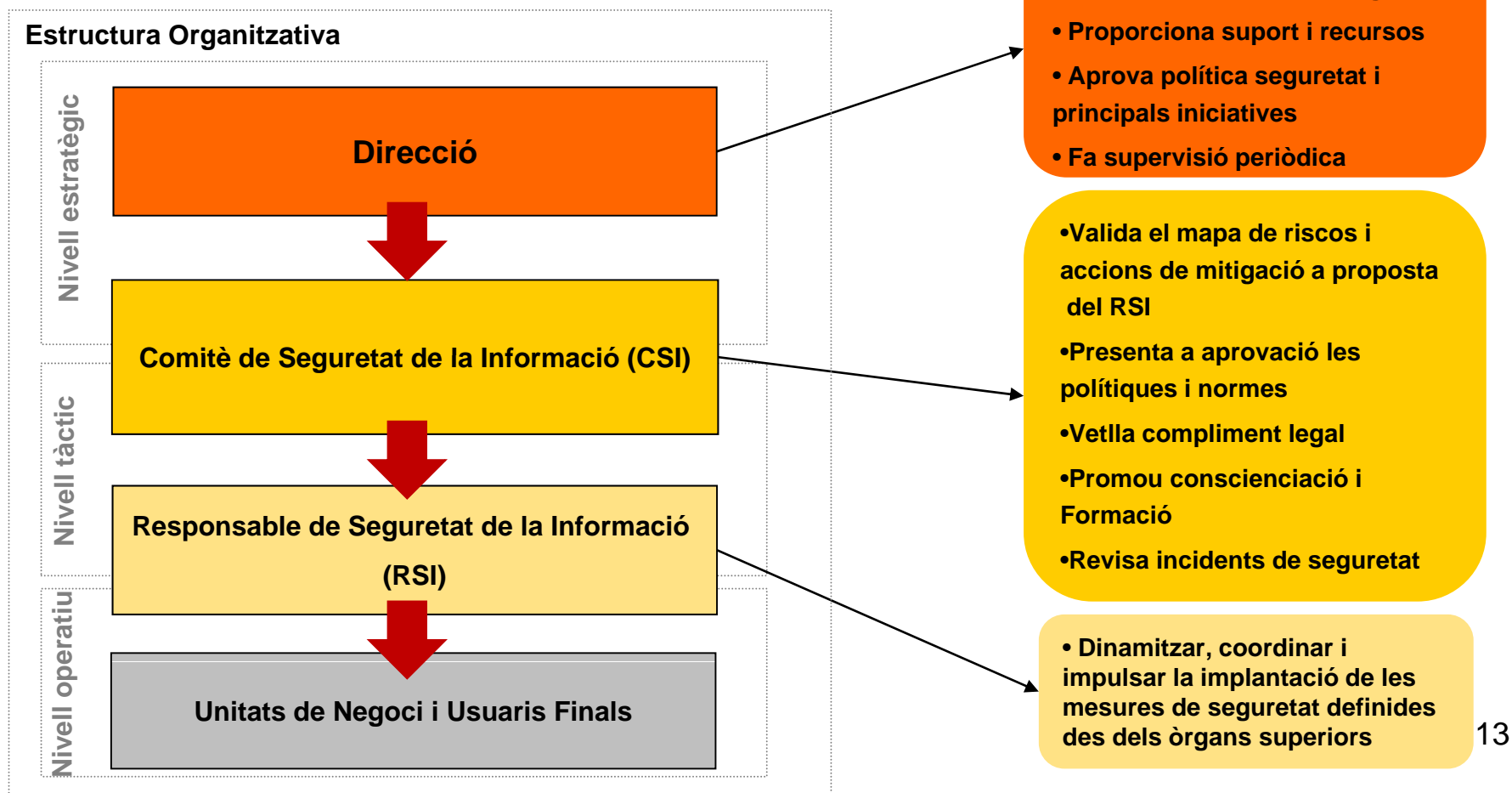
- Proposar accions de millora i mitigació del risc.
- Implantar les mesures de seguretat definides des dels nivells tàctics i estratègics.

Construint una Estructura Organitzativa de Seguretat



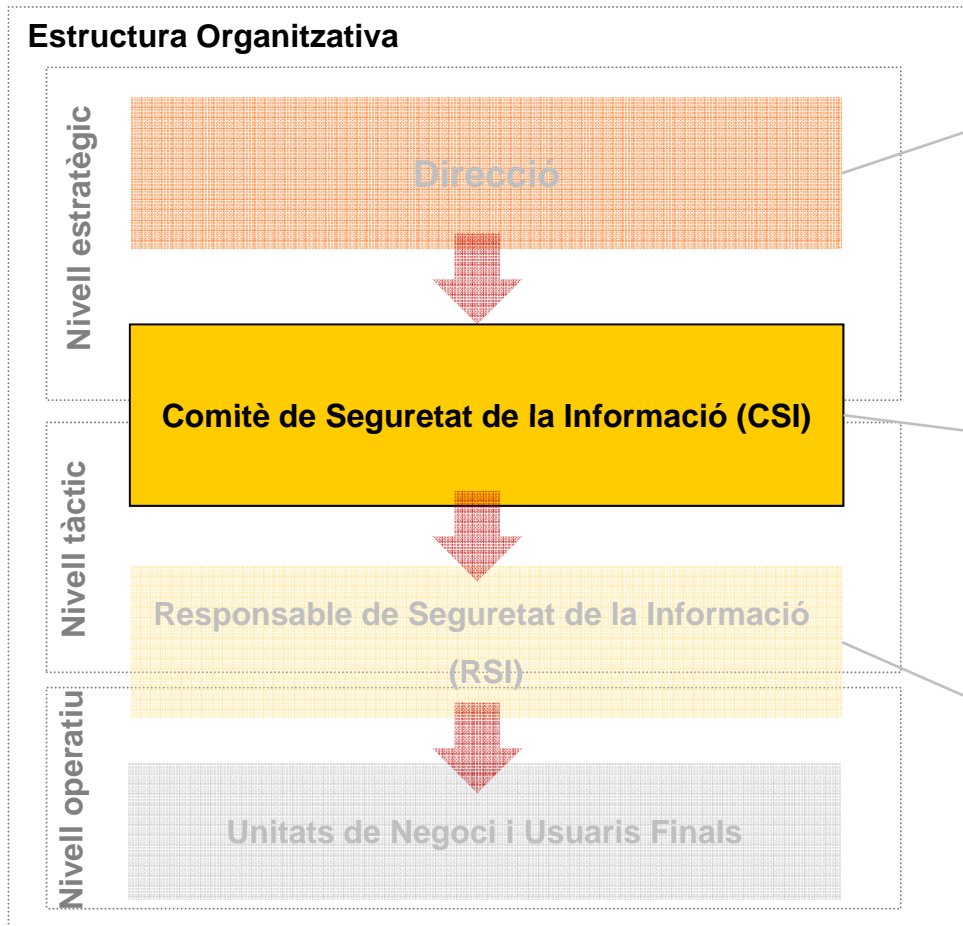
Construint una Estructura Organitzativa de Seguretat

Com es relacionen i quines funcions tenen?



Construint una Estructura Organitzativa de Seguretat

Com es relacionen i quines funcions tenen?



- Visió estratègica
- Nomena un Comitè de Seguretat
- Proporciona suport i recursos
- Aprova política seguretat i principals iniciatives
- Fa supervisió periòdica

Factor Crític d'èxit: Elecció dels membres del CSI

- Valora el context legal
- Promou conscienciació i Formació
- Revisa incidents de seguretat

- Dinamitzar, coordinar i impulsar la implantació de les mesures de seguretat definides des dels òrgans superiors

Construint un CSI

Criteris en l'elecció dels seus components

- Equilibri dels membres que el componen de forma que quedi representada:

- Part Tècnica.>
- Part Organitzativa.>
- Àrees de negoci.>

✓ Resp. de SSII/ Director TIC: Viabilitat Tècnica.
✓ RSI: Punt focal en seguretat de la informació.
✓ Resp. de Seguretat Física.

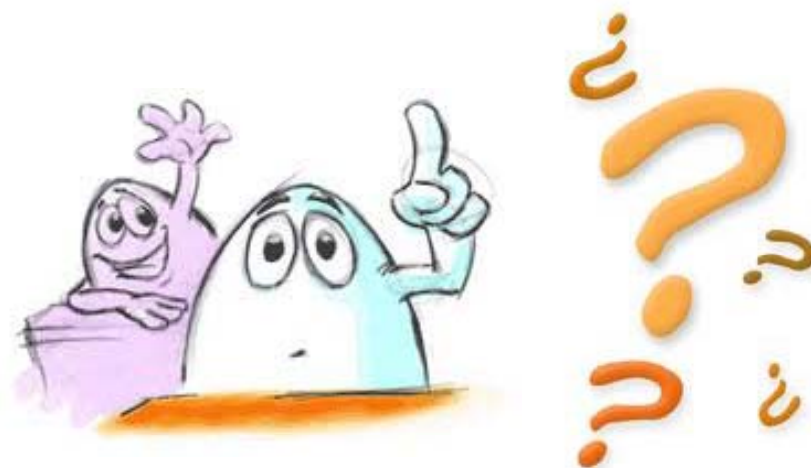
✓ Resp. / Directors de les àrees de negoci amb informació més crítica o bé processos amb riscos més elevats: Alineació requeriments amb el negoci.

✓ Àrea de RRHH /Organització: Gestió del canvi.
✓ Assessoria Jurídica: Compliment legal.
✓ Control Intern: auditoria interna.

Construint un CSI

Criteris en l'elecció dels seus components

- Acotar el nombre de membres que el componen
 - Facilitarà el consens entre el components de les iniciatives que pujaran a aprovació (polítiques, normes, mapa de riscos, etc.).
- Capacitat de presa de decisió dels membres.
 - Legitimació.
- Visió transversal.
 - Garantir el coneixement ampli de l'organització.
- Tots els membres del CSI haurien d'estar al mateix nivell jeràrquic dins de l'organització.
- Contemplar la possibilitat de membres permanents i d'altres convidats puntualment.
 - En base als temes a tractar pot ser recomanable convidar a especialistes en la matèria.
- No intentar aprofitar estructures existents en l'organització.
 - Acostuma a identificar-se mancances en les funcions bàsiques en l'àmbit de la seguretat.



Preguntes?



Alguna Pregunta Més?