SGSI:Cotecom

Nom Estudiant: Esteve Grassot Roselló

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Nom Consultor: Arsenio Tortaja Gallego

Centre: UOC

Data Lliurament:
23/12/14

Llicències alternatives (triar alguna de les següents i substituir la de la pàgina anterior)

A) Creative Commons:

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-CompartirIgual 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-SenseObraDerivada 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement-CompartirIgual 3.0 Espanya de Creative Commons

Aquesta obra està subjecta a una llicència de Reconeixement 3.0 Espanya de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FITXA DEL TREBALL FINAL

Títol del treball:	*SGSI:Cotecom*
Nom de l'autor:	*Esteve Grassot Roselló*
Nom del consultor:	*Arsenio Tortaja Gallego*
Data de lliurament (mm/aaaa):	*MM/AAAA*
Àrea del Treball Final:	*Sistemes gestió seguretat informació*
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

Implantació d'un Sistema de Gestió de la Seguretat Informàtica, que cobreixi el seu personal, equips informàtics, el CPD, la sala de comunicacions, copies de seguretat, armaris de xarxa, electrònica de xarxa, servidors, serveis i dades de Cotecom.

L'objectiu és desenvolupar un pla o full de ruta que ha de seguir l'empresa per a gestionar i analitzar de forma adequada la seguretat, permetent, no només conèixer l'estat d'aquesta, les seves mancances i riscos, sinó també les línies on s'ha d'actuar per millorar-la, implantant un model de millora continua PDCA. Tot plegat per establir les bases d'un Pla director de seguretat per a Cotecom.

Entre algunes de les tasques més importants del projecte, caldrà:

- Estudiar la situació actual de Cotecom.
- Identificar les amenaces que l'organització o que l'empresa té o hi està exposada, i el seu impacte present i futur.
- Inventariar els actius de l'empresa, realitzant un inventari i classificant cada tipus d'actiu.
- Documentar la normativa de seguretat de la informació de l'empresa.
- Descriure els riscos de Cotecom en els diferents elements o actius.
- Proposar accions o projectes a realitzar per solucionar les possibles mancances o riscos.
- Avaluar les millores realitzades i oferir els resultats envers l'anterior situació, per obtenir-ne conclusions.

Abstract (in English, 250 words or less):

Implementation of a management system for information security that covers their personal computers, the CPD, the communications room, backups, network cabinets, network electronics, servers, services and data of Cotecom.

The objective is to develop a plan or roadmap to be followed by the company to manage and analyze adequately the security, allowing not only to know the status of this, its shortcomings and risks, but also lines which must act to improve it, implementing a continuous improvement model PDCA. Everything to lay the foundations of a Master Plan for security Cotecom.

Some of the most important tasks of the project will:

• Study the current situation of Cotecom.

• Identify threats to the organization or company that has or is exposed there, and its present and future impact.

• Inventory of the assets of the company, making an inventory and classifying each type of asset.

• Document the rules of information security company.

• Describe the risks of the different elements Cotecom or assets.

• Propose actions or projects to do to address the deficiencies or potential risks.

• Evaluate the improvements and provide results regarding the above situation, to obtain conclusions.

Paraules clau (entre 4 i 8):

SGSI, Seguretat, informació, anàlisis, riscos

Índex de continguts

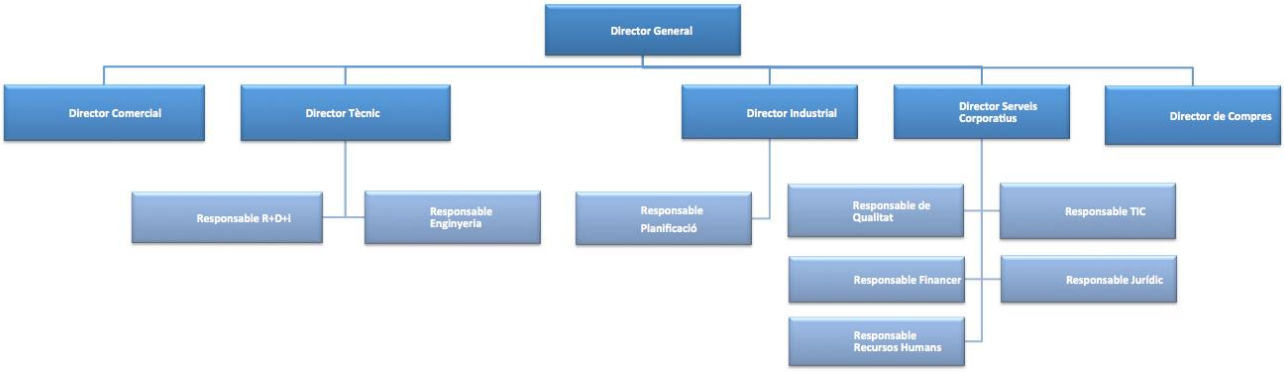
Situació actual Cotecom

Per raons de confidencialitat, algunes dades de seguretat analitzades i el propi nom de l'empresa - substituït per Cotecom - no podran ser revelats en aquest projecte, evitant així comprometre la seguretat i confidencialitat de les dades, infraestructura i anonimat dels treballadors.

Cotecom és una multinacional dedicada a la fabricació de maquinària per impressió i conversió de l'envàs flexible. Actualment està formada per uns 500 treballadors, amb tres seus situades a Brasil, Itàlia i Girona. A l'actualitat hi estic desenvolupant tasques com a Administrador de Sistemes i Comunicacions i gestió dels projectes de millora d'aquests entorns.

A dia d'avui no hi ha establerta cap política sobre la seguretat informàtica de l'empresa, exceptuant les 4 directrius bàsiques sobre el bon ús de la informació i gestió de contrasenyes, per això la meva motivació a realitzar aquest projecte d'implantació d'un Sistema de Gestió de la Seguretat Informàtica (SGSI) que permeti regularitzar aquesta situació i adequar-la a la ISO/IEC 27001+ISO/IEC 27002.

A continuació es pot veure l'organigrama directiu de Cotecom, no s'entra en detall ja que simplement ha de servir per a fer-se una idea de com està organitzada l'empresa.



Cotecom no ofereix cap servei més enllà dels lligats amb el seu producte com a servei post venda (revisions, manteniments, garantia, avaries...), ja que la seva finalitat principal com a empresa es la fabricació de bens d'equip pel sector de l'embalatge flexible. Els serveis informàtics són d'ús intern.

Actualment des de TIC no es disposa d'un departament de seguretat específic, sinó que la seguretat forma part del departament. Aquest vetlla per tenir cobert aquest àmbit de la millor manera possible, a més de desenvolupar altres tasques pròpies del departament.

Els usuaris treballen amb diferents perfils d'equipament, sobretaules, estacions de treball, portàtils tècnics i portàtils lleugers, tots ells amb Windows 7 o 8.1, la plataforma ofimàtica de Microsoft office 2010 o 2013 i el ESET Nod32 com a sistema antivíric. També disposen de terminals Android agregats com a eina d'empresa a Google Apps des d'on es gestionen. En tots els casos anteriors són els propis usuaris que s'administren els ordinadors o smartphones, i tenen el suport de Helpdesk en cas de incidències.

Com a principals serveis corporatius interns tenim ERP SAP, gestió de producte PLM – Windchill, A3 per a la gestió de nòmines, Google apps per al correu i comunicació, Alfresco per a gestió documental no relacionada amb producte i samba com a repositori de fitxers. En tots els casos son serveis interns per als treballadors de Cotecom i en cas d'accedir des de l'exterior cal utilitzar la connexió VPN.

Aquets serveis estan localitzats en el CPD i funcionen en una plataforma VMWare 5.5U1 amb un clúster de 4 hosts i dos armaris de discos, el CPD està protegit amb aires condicionats, SAI's i sistema antiincendis.

Per altre banda el servei de xarxa està en una altre sala anomenada Sala de Comunicacions, on hi ha l'entrada principal de les línies de comunicacions, firewalls i equipament de xarxa, també protegida amb SAI's i aires condicionats.

Abast

L'Abast d'aquest projecte és la implantació d'un Sistema de Gestió de la Seguretat Informàtica a la seu de Girona, que cobreixi el seu personal, equips informàtics, el CPD, la sala de comunicacions, copies de seguretat, armaris de xarxa, electrònica de xarxa, servidors, serveis i dades de Cotecom.

- Personal: Personal contractat per Comexi que treballen per a l'empresa, tant des de les seves instal·lacions com des de fora d'aquestes, ja sigui des de casa del client, proveïdor, hotel o teletreball.
- Equips Informàtics: Eines amb les quals el personal desenvolupa les seves feines, PDA, equips sobre taula, portàtils, smartphones, tauletes i impressores,
- CPD: Centre de processament de dades, lloc on hi ha els servidors, serveis i dades de l'empresa.
- Sala de comunicacions: Sala on es troben les entrades de comunicacions de l'empresa (ADSL, Fibra òptica), tallafocs i electrònica de xarxa.
- Armaris de xarxa: Armaris que contenen l'electrònica de xarxa, i donen servei als equips informàtics.
- Servidors: Equips que proporcionen els serveis de l'empresa i les seves dades.
- Serveis: Eines corporatives com el SAP, Gestor documental, PLM, servidor de fitxers, servei DNS...
- Copies de seguretat: Medis d'emmagatzematge que contenen dades de l'empresa.

Objectius

L'objectiu és desenvolupar un pla o full de ruta que ha de seguir l'empresa per a gestionar i analitzar de forma adequada la seguretat, permetent, no només conèixer l'estat d'aquesta, les seves mancances i riscos, sinó també les línies on s'ha d'actuar per millorar-la, implantant un model de millora continua PDCA. Tot plegat per establir les bases d'un Pla director de seguretat per a Cotecom.

Entre algunes de les tasques més importants del projecte, caldrà:

- Estudiar la situació actual de Cotecom.
- Identificar les amenaces que l'organització o que l'empresa té o hi està exposada, i el seu impacte present i futur.

- Inventariar els actius de l'empresa, realitzant un inventari i classificant cada tipus d'actiu.
- Documentar la normativa de seguretat de la informació de l'empresa.
- Descriure els riscos de Cotecom en els diferents elements o actius.
- Proposar accions o projectes a realitzar per solucionar les possibles mancances o riscos.
- Avaluar les millores realitzades i oferir els resultats envers l'anterior situació, per obtenir-ne conclusions.

Auditoria Prèvia

Com a punt de partida s'ha realitzat un anàlisis per determinar quines són les àrees de millora que s'haurien d'aplicar segons la Norma ISO/IEC 27002/2013, que engloba 14 dominis, 35 objectius de control i 114 controls.

CONTROL				**Compleix**
A.5 Política de Seguretat de la Informació				
	A.5.1 Directrius de la Direcció en seguretat de la informació			
		A.5.1.1	Conjunt de polítiques per la seguretat de la informació	Existeix un document de polítiques de seguretat disponible per tots els usuari?	NO
		A.5.1.2	Revisió de les polítiques per la seguretat de la informació	Es fan revisions regulars de la política de seguretat?	NO
A.6 Organització de la Seguretat de la Informació				
	A.6.1 Organització interna			
		A.6.1.1	Assignació de responsabilitats per la seguretat de la informació	Estan definides les responsabilitats per protegir i controlar la informació i els sistemes?	NO
		A.6.1.2	Segregació de tasques	Estan segregades les tasques per a millor control de l'entorn?	NO
		A.6.1.3	Contacte amb les autoritats	L'empresa manté contacte amb autoritats especialistes de seguretat?	NO
		A.6.1.4	Contacte amb grups d'interès especial	L'empresa pertany a grups d'interès, fòrums o associacions de seguretat externs?	NO
		A.6.1.5	Seguretat de la informació en la gestió de projectes	Estan definides les mesures de la seguretat de la informació en la gestió de projectes?	NO
	A.6.2 Dispositius mòbils i teletreball			
		A.6.2.1	Política d'us de dispositius mòbils	Existeix una política i controls per la protecció contra el risc de treballar amb dispositius mòbils?	NO
		A.6.2.2	Teletreball	Existeix una política i procediments per autoritzar i controlar les activitats de teletreball?	NO
A.7 Seguretat dels Recursos humans				
	A.7.1 Abans de la contractació			
		A.7.1.1	Investigació d'antecedents	Es realitza una investigació d'antecedents del personal a contractar?	NO
		A.7.1.2	Termes i condicions de contractació	Estan establertes les responsabilitats relatives a la seguretat en termes i condicions del contracte de treball?	NO

A.7.2 Durant la contractació				
	A.7.2.1	Gestió de les responsabilitats	S'assegura que les responsabilitats de seguretat de cada un són aplicades?	NO
	A.7.2.2	Conscienciació, educació i capacitació en Seg. de la informació	Els treballadors i usuaris de terceres parts reben la formació apropiada, relativa a polítiques i procediments?	NO
	A.7.2.3	Procés disciplinari	Existeix un procés disciplinari per tractar les violacions realitzades per els treballadors de les polítiques i procediments de seguretat?	SI
A.7.3 Cessament o canvi de lloc de treball				
	A.7.3.1	Cessament o canvi de lloc de treball	S'assegura la retirada dels drets d'accés dels treballadors i usuaris de terceres parts al seu cessament o canvi de lloc de treball?	NO
A.8 Gestió d'actius				
A.8.1 Responsabilitat sobre els actius				
	A.8.1.1	Inventari d'actius	Existeixen i es mantenen actualitzats inventaris dels actius del sistema d'informació?	SI
	A.8.1.2	Propietat dels actius	S'han designat els propietaris de tots els actius del sistema d'informació?	NO
	A.8.1.3	Us acceptable dels actius	Estan definits i documentades les regles de l'ús acceptable d'actius de sistemes de la informació?	NO
	A.8.1.4	Devolució dels actius	S'assegura la devolució de tots els actius de l'organització en possessió dels treballadors i usuaris de terceres parts a la finalització de la contractació?	NO
A.8.2 Classificació de la informació				
	A.8.2.1	Directrius de classificació	Existeix un esquema per classificar la informació i els sistemes en funció de la seva confidencialitat o importància?	NO
	A.8.2.2	Etiquetat i manipulat de la informació	Existeixen procediments per identificar i fer servir la informació en base als esquemes de classificació?	NO
	A.8.2.3	Manipulació dels actius	Existeix alguna guia o procediment de manipulació d'actius?	NO
A.8.3 Utilització de suports d'emmagatzematge				
	A.8.3.1	Gestió de suports extraïbles	Hi ha procediments per gestionar suports extraïbles amb informació com discs, CD's, informes, impresos, ...?	NO
	A.8.3.2	Eliminació de suports	S'han desenvolupat procediments per assegurar el fitxer i la destrucció dels suports informàtics?	SI
	A.8.3.3	Suports físics en transit	Es pren alguna mesura especial amb els suports en trànsit amb informació sensible?	NO
A.9 Control d'accés				
A.9.1 Requisits del negoci per el control d'accés				

		A.9.1.1	Política de control d'accessos	Estan documentades les regles i els drets d'accés dels usuaris i grups?	NO
		A.9.1.2	Control d'accés a les xarxes i serveis associats	Existeix algun control d'accés a les xarxes i serveis associats?	SI
	A.9.2 Gestió d'accés d'usuari				
		A.9.2.1	Gestió d'altes/baixes en el registre d'usuaris	Queden registrats els accessos dels usuaris?	SI
		A.9.2.2	Gestió dels drets d'accés assignats a usuaris	Està controlada la gestió dels drets d'accés?	SI
		A.9.2.3	Gestió dels drets d'accés amb privilegis especials	Està controlada la gestió dels drets d'accés amb privilegis especials?	SI
		A.9.2.4	Gestió de informació confidencial d'autenticació d'usuaris.	Es controla la gestió de la informació confidencial referent a l'autenticació dels usuaris?	NO
		A.9.2.5	Revisió dels drets d'accés dels usuaris.	Es revisen periòdicament els drets d'accés dels usuaris?	SI
		A.9.2.6	Retirada o adaptació dels drets d'accés	S'assegura la retirada dels drets d'accés dels treballadors i usuaris de terceres parts a la finalització de la contractació o acord?	SI
	A.9.3 Responsabilitat dels Usuaris				
		A.9.3.1	Us de la informació confidencial per l'autenticació	S'explica la responsabilitat de l'ús de la informació confidencial per a l'autenticació a els usuaris?	NO
	A.9.4 Control d'accés a sistemes i aplicacions				
		A.9.4.1	Restricció d'accés a la informació	Està restringit l'accés a la informació i funcions dels sistemes d'aplicació?	SI
		A.9.4.2	Procediments segurs d'inici de sessió	Existeixen procediments que expliquin com realitzar inicis de sessió segurs?	NO
		A.9.4.3	Gestió de contrasenyes d'usuari	Existeix algun procés per la gestió de contrasenyes?	NO
		A.9.4.4	Us d'eines d'administració de sistemes	S'utilitzen eines per a l'administració i control dels sistemes informàtics?	NO
		A.9.4.5	Control d'accés al codi font dels programes	Existeix un control d'accés al codi font dels programes?	SI
A.10 Criptografia					
	A.10.1 Xifrat				
		A.10.1.1	Política d'us dels controls criptogràfics	Existeix una política que defineixi l'ús de controls de xifrat per la protecció de la informació?	NO
		A.10.1.2	Gestió de contrasenyes	S'utilitza algun sistema de gestió de les claus per suportar l'ús de les tècniques criptogràfiques?	NO
A.11 Seguretat física i de l'entorn					
	A.11.1 Àrees segures.				
		A.11.1.1	Perímetres de seguretat física.	Existeix un perímetre de seguretat per protegir les àrees on estan els sistemes?	SI
		A.11.1.2	Controls físics d'entrada.	Estan les àrees protegides per controls d'entrada, per permetre l'accés només al personal autoritzat?	NO
		A.11.1.3	Seguretat d'oficines, despatxos i recursos.	Estan protegides les oficines, despatxos i recursos que tenen algun requeriment de seguretat especial?	NO
		A.11.1.4	Protecció contra les amenaces externes i	Estan protegides les àrees de	SI

			ambientals.	seguretat contra incendis, inundacions, terratrèmols, explosions, disturbis i altres formes de desastres naturals o origen humà?	
		A.11.1.5	El treball en àrees segures.	Existeixen controls físics especials per treballar en les àrees segures?	NO
		A.11.1.6	Àrees d'accés públic, carga i descarrega.	Estan les àrees d'entrada i sortida de mercaderies aïllades de l'àrea de sistemes?	NO
	A.11.2 Seguretat dels equips				
		A.11.2.1	Localització i protecció d'equips.	Estan els equips situats o protegits per reduir les opcions d'accés no autoritzat?	NO
		A.11.2.2	Instal·lacions de subministres.	Estan protegits els equips contra fallades de subministrament (llum, aigua, calefacció, aire condicionat, clavegueram)?	SI
		A.11.2.3	Seguretat del cablejat.	Estan protegits contra danys o escoltes els cables que transmeten dades o suporten serveis d'informació?	SI
		A.11.2.4	Manteniment dels equips.	Es mantenen els equips en base a les recomanacions del fabricant i/o procediments documentats?	SI
		A.11.2.5	Sortida d'actius fora de les dependències de l'empresa	Es necessita una autorització per treure de les oficines equips, informació o software?	NO
		A.11.2.6	Seguretat dels equips i actius fora de les instal·lacions.	Existeixen procediments de seguretat i que cobreixin la seguretat dels sistemes quan s'utilitzen fora de les premisses de l'empresa?	NO
		A.11.2.7	Reutilització o retirada segura dels dispositius d'emmagatzematge	Es borra la informació dels equips o dispositius d'emmagatzematge abans de reutilitzar-los o retirar-los?	SI
		A.11.2.8	Equip informàtic d'usuari desatès.	Es sol·licita als usuaris adoptar mesures de protecció amb els equips desatesos?	NO
		A.11.2.9	Política de lloc de treball net i bloqueig de pantalla	Existeix una política de pantalles i lloc de treball net per els entorns de treball?	NO
A.12 Seguretat en les operacions					
	A.12.1 Responsabilitat i procediments d'operació				
		A.12.1.1	Documentació de procediments d'operació.	Estan documentats i mantinguts els procediments operacionals?	NO
		A.12.1.2	Gestió de canvis.	Estan controlats els canvis dels sistemes i aplicacions?	SI
		A.12.1.3	Gestió de capacitats.	Estan gestionades les capacitats per reduir l'oportunitat de mals usos dels sistemes?	NO
		A.12.1.4	Separació d'entorns de desenvolupament, prova i producció.	Estan separades les àrees de desenvolupament i prova de les dels sistemes en operació?	SI
	A.12.2 Protecció contra codi maliciós.				
		A.12.2.1	Controls contra codi maliciós.	Existeixen procediments implantats per protegir a l'empresa contra codi maliciós?	SI
	A.12.3 Copies de seguretat.				

A.12.3.1	Copies de seguretat de la informació.	Es fan regularment copies de seguretat de la informació?	SI
A.12.4 Registre de l'activitat i supervisió.			
A.12.4.1	Registre i gestió d'esdeveniments d'activitat.	Existeixen procediments per monitoritzar l'ús de serveis de processos de la informació?	SI
A.12.4.2	Protecció dels registres d'informació.	Estan protegits contra manipulació i accés no autoritzat els registres de sistemes de la informació?	SI
A.12.4.3	Registres d'activitat de l'administrador i operador de sistemes.	Es registren i revisen regularment les activitats dels administradors i operadors de sistemes?	NO
A.12.4.4	Sincronització de rellotges.	Estan sincronitzats tots els rellotges dels ordinadors?	SI
A.12.5 Control del software en explotació			
A.12.5.1	Instal·lació del software en sistemes en explotació	S'aplica algun control per implantar software en el sistema en operació?	NO
A.12.6 Gestió de la vulnerabilitat tècnica.			
A.12.6.1	Gestió de les vulnerabilitats tècniques.	Es gestionen, analitzen i corregeixen les vulnerabilitats tècniques dels sistemes?	NO
A.12.6.2	Restriccions en la instal·lació de software.	Està restringida o controlada la instal·lació de software?	NO
A.12.7 Consideracions de les auditories dels sistemes d'informació.			
A.12.7.1	Controls d'auditoria dels sistemes d'informació.	Estan planificades les auditories de sistemes per reduir el risc d'interrupcions en el procés de negoci?	NO
A.13 Seguretat en les comunicacions			
A.13.1 Gestió de la seguretat en les xarxes			
A.13.1.1	Controls de xarxa	S'han implantat algun tipus de control per mantenir la seguretat de la xarxa?	SI
A.13.1.2	Mecanismes de seguretat associats a els serveis de xarxa.	Estan documentats els atributs de seguretat de tots els serveis de xarxa?	NO
A.13.1.3	Segregació de Xarxes	Existeix una segregació de xarxes segons les necessitats de cada una?	SI
A.13.2 Intercanvi d'informació amb parts externes.			
A.13.2.1	Polítiques i procediments d'intercanvi d'informació.	Estan documentades les polítiques, procediment i mesures per intercanvi d'informació a través de tots els tipus formes de comunicació?	NO
A.13.2.2	Acords d'intercanvi.	S'han establert acords amb altres empreses per intercanviar informació o aplicacions?	SI
A.13.2.3	Missatgeria electrònica.	Està protegit el comerç electrònic contra activitats fraudulentes?	NO
A.13.2.4	Acords de confidencialitat i secret	Es firmen acords de confidencialitat amb intercanvi d'informació amb parts externes?	SI
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.			
A.14.1 Requisits de seguretat dels sistemes d'informació.			
A.14.1.1	Anàlisis i especificacions dels requisits de seguretat.	S'han especificat els controls de seguretat necessaris per nous	NO

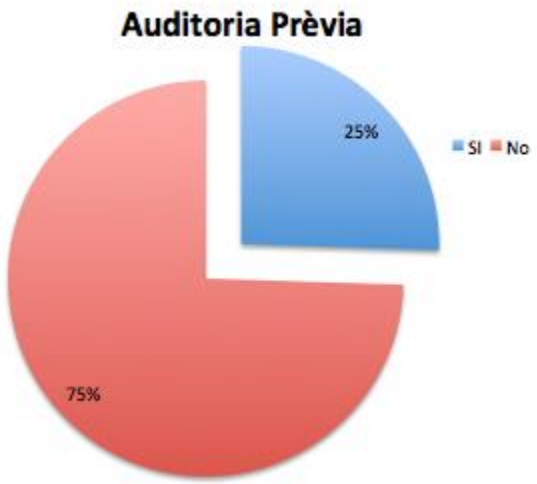
				sistemes o millores dels actuals?	
		A.14.1.2	Seguretat en les comunicacions en serveis accessibles per xarxes publiques.	Estan assegurades les comunicacions a serveis quan s'accedeix des de xarxes públiques?	NO
		A.14.1.3	Protecció de les transaccions per xarxes de comunicacions.	S'estableix alguna protecció en les transaccions que es realitzen mitjançant xarxes de comunicacions?	SI
	A.14.2 Seguretat ens els processos de desenvolupament i suport				
		A.14.2.1	Polítiques de desenvolupament segur de software.	S'ha establert una política de desenvolupament segur de software?	NO
		A.14.2.2	Procediments de control de canvis en els sistemes.	Hi ha un procediment de control de canvis o versions en els sistemes o programes informàtics?	NO
		A.14.2.3	Revisió tècnica de les aplicacions després de fer canvis en el SO.	Es realitza una revisió tècnica després de realitzar canvis?	SI
		A.14.2.4	Restriccions en els canvis en els paquets de software.	Hi ha una política de restriccions en els canvis en els paquets de software?	SI
		A.14.2.5	Us de principis d'enginyeria en protecció de sistemes.	S'utilitzen principis d'enginyeria en la protecció de sistemes?	NO
		A.14.2.6	Seguretat en entorns de desenvolupament	S'utilitzen mètodes de seguretat en l'accés a entorns de desenvolupament?	SI
		A.14.2.7	Externalització del desenvolupament de software	Està procedimentat, controlat i verificat l'externalització del desenvolupament de software?	NO
		A.14.2.8	Proves de funcionalitat durant el desenvolupament de sistemes	Es realitzen proves de funcionalitat durant els desenvolupament de sistemes?	SI
		A.14.2.9	Proves d'acceptació.	Es realitzen proves d'acceptació dels desenvolupaments?	NO
	A.14.3 Prova de dades				
		A.14.3.1	Protecció de les dades utilitzades en proves.	Es protegeixen les dades utilitzades en les proves?	SI
A.15 Relació amb els proveïdors					
	A.15.1 Seguretat de la informació en les relacions amb proveïdors.				
		A.15.1.1	Política de seguretat de la informació per proveïdors.	S'ha establert una política de seguretat de la informació per a proveïdors?	NO
		A.15.1.2	Tractament del risc dintre d'acords de proveïdors.	Existeix un document que tracti el risc dintre dels acord de proveïdors de sistemes informàtics?	NO
		A.15.1.3	Cadena de subministrament en tecnologies de la informació i comunicacions.	Està controlada la cadena de subministrament en tecnologies de la informació i comunicació?	NO
	A.15.2 Gestió de la prestació del servei per proveïdors.				
		A.15.2.1	Supervisió i revisió dels serveis prestats per tercers.	Es realitza una supervisió i supervisió dels serveis prestats per tercers?	NO
		A.15.2.2	Gestió de canvis en els serveis prestats per tercers.	Existeix una gestió de canvis en els serveis prestats per tercers?	NO
A.16 Gestió de incidències de seguretat de la informació					
	A.16.1 Gestió de incidències de seguretat de la informació				
		A.16.1.1	Responsabilitats i procediments.	S'han establert procediments i responsabilitats, per la gestió	NO

				d'incidents?	
		A.16.1.2	Notificació dels esdeveniments de seguretat de la informació.	Existeix un canal a través del qual es reportin els incidents de seguretat?	NO
		A.16.1.3	Notificació dels punts dèbils de la seguretat.	Es sol·licita a els usuaris que comuniquin qualsevol debilitat de seguretat o amenaça pel sistema?	NO
		A.16.1.4	Valoració dels esdeveniments de seguretat de la informació i pressa de decisions.	Es valoren i es pren una decisió sobre els esdeveniments de seguretat de la informació?	SI
		A.16.1.5	Resposta a els incidents de seguretat.	Es corregeixen els incidents de seguretat?	SI
		A.16.1.6	Aprenentatge dels incidents de seguretat informàtica.	Existeixen mecanismes que funcionen per realitzar anàlisis del tipus, volum i cost de les incidències i errades?	SI
		A.16.1.7	Recopilació d'evidències.	Per recolzar una acció contra una persona o organització, es mantenen les evidencies, conforme a les lleis i normes publicades?	NO
A.17 Els aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci.					
	A.17.1 Continuïtat de la seguretat de la informació				
		A.17.1.1	Planificació de la continuïtat de la seguretat de la informació.	Existeix un pla estratègic, basat en la valoració de risc, on es detallin les accions per la continuïtat del negoci?	NO
		A.17.1.2	Implantació de la continuïtat de la seguretat de la informació.	Estan desenvolupats els plans de continuïtat per mantenir o restaurar les operacions del negoci en un temps raonable?	NO
		A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	Es verifiquen, revisen i avaluen regularment els plans de continuïtat de negoci per assegurar que són eficaços?	NO
	A.17.2 Redundàncies				
		A.17.2.1	Disponibilitat d'instal·lacions per el processament de la informació.	Existeixen redundàncies en la disponibilitat d'instal·lacions del processament de la informació, que permetin suportar talls d'energia elèctrica, aigua, comunicacions..?	SI
A.18 Compliment					
	A.18.1 Compliment dels requeriments legals i contractuals.				
		A.18.1.1	Identificació de la legislació aplicable.	Estan definits i documentats per cada sistema d'informació tots els requeriments contractuals, reguladors i estatutaris?	NO
		A.18.1.2	Drets de propietat intel·lectual (DPI).	Hi ha procediments per assegurar el compliment amb les restriccions legals en l'ús de material referent a els drets de la propietat intel·lectual?	NO
		A.18.1.3	Protecció dels registres de l'organització.	Estan protegits contra pèrdua, destrucció i falsificació els registres importants?	NO
		A.18.1.4	Protecció de dades i privacitat de la informació personal.	Existeixen controls eficaços, per protegir la informació personal en base a la legislació vigent?	SI
		A.18.1.5	Regulació dels controls criptogràfics.	Existeixen controls per assegurar el	NO

				compliment amb els acords nacionals per controlar l'ús de xifrat?	
	A.18.2 Revisions de la seguretat de la informació.				
		A.18.2.1	Revisió independent de la seguretat de la informació.	Existeix algun control/auditoria independent/externa de la seguretat de la informació?	NO
		A.18.2.2	Compliment de les polítiques i normes de seguretat.	Assegura la direcció que s'estan seguint correctament els procediments de seguretat, dintre de la seva àrea de responsabilitat?	NO
		A.18.2.3	Comprovació del compliment.	Es revisen regularment els sistemes d'informació per verificar el compliment amb els estàndards d'implantació de seguretat?	NO

Valoració auditoria prèvia

Com s'ha pogut veure en l'auditoria prèvia, Cotecom només compleix en 39 dels 114 controls de la Norma ISO/IEC 27002/2013. Tal com es veu en la següent imatge un 25% compleix amb la Norma i el 75% no la compleix, per tant aquest 75% es l'objecte de millora del SGSI.



Política de seguretat

Introducció

Tots els Sistemes de Gestió es recolzen en un cos documental pel compliment normatiu. En aquesta fase es desenvoluparà el sistema de gestió documental que s'utilitzarà en el nostre Sistema de Gestió de la Seguretat de la Informació. Aquest sistema contindrà una sèrie de documents que venen establerts a la pròpia norma ISO/IEC 27001.

En aquest document s'especifica la normativa interna o la política de seguretat que pot tenir l'organització, i que els diferents perfils de treballadors de l'organització han de conèixer i complir degudament. S'especifiquen els termes relatius a l'accés a la informació, els recursos, o com actuar davant incidents.

La política de seguretat contemplarà què entén Cotecom per seguretat de la informació i l'ús adequat de tots els recursos tecnològics per part dels diferents perfils d'usuaris, en referencia a la confidencialitat, integritat, disponibilitat, autenticitat, privacitat i traçabilitat de la informació de Cotecom.

Objectius de la política de seguretat

L'objectiu de la política de seguretat de la informació és establir les directrius en seguretat de la informació, alineades amb els objectius del negoci i la legislació aplicable, tot plegat confirmat i amb el compromís de la direcció de Cotecom.

Aquestes directrius en seguretat han de poder ser seguides per tot el personal de Cotecom, i terceres persones o empreses que tinguin una relació amb Cotecom, per tal de mantenir segurs els sistemes de seguretat de l'empresa, intentant minimitzar els riscos, assegurant una disponibilitat, confidencialitat i integritat de totes les dades i sistemes de l'empresa, i en la normativa vigent corresponent a la LOPD (Llei Orgànica de Protecció de Dades).

La política es posarà en funcionament un cop l'empresa accepti la política de seguretat i un cop tot el seu personal hagi estat format i documentat, això inclou a terceres parts (clients, proveïdors, col·laboradors, etc.) que puguin utilitzar els sistemes d'informació de Cotecom.

També cal esmentar que aquetes directrius, com la resta de normes, procediments, estàndards o qualsevol document relacionat amb la seguretat de la informació i les dades que tracten de caràcter confidencial, només està permès el seu ús i difusió en caràcter intern i per personal autoritzat.

Polítiques a desenvolupar

Política general de l'organització: Estableix un conjunt de normatives o polítiques aplicables a tota l'organització, revisades, controlades i millorades per el comitè de seguretat de Cotecom.

Política de gestió de recursos humans: S'han d'assignar responsabilitats sobre la seguretat prèvia a la contractació i definir adequadament el lloc de treball i els termes i condicions de la contractació. També caldrà fer una correcta investigació dels candidats i si són contractats hauran de signar un compromís sobre les seves funcions i responsabilitats relatives al seu lloc de treball.

Finalment, s'ha d'establir com el treballador ha de sortir de l'empresa de manera que es garanteixi la completa devolució de tots els equips i recursos assignats, retirada de drets d'accés lògics i físics als sistemes d'informació de Cotecom.

Política de gestió d'actius: Definició de com s'han inventariar tots els actius de Cotecom, com identificar els seus propietaris i assignar les responsabilitats del manteniment dels controls adequats. La informació ha de ser classificada per indicar la seva necessitat, prioritat i el grau esperat de protecció quan es treballa amb la informació. Cal definir un conjunt de nivells de protecció i comunicar la necessitat de les mesures especials de tractament.

Aquest domini de controls es essencial per poder realitzar l'anàlisi de risc, ja que si no identifiquem i classifiquem els actius, es impossible valorar-los i calcular el seu risc.

Política de control d'accessos: Estableix la gestió de manera segura l'accés dels usuaris als sistemes d'informació, per prevenir un ús no autoritzat. Cal definir procediments formals per controlar l'assignació dels drets d'accés que cobreixin els procediments del cicle de vida de l'usuari, des de la seva alta al sistema a la seva baixa a Cotecom o canvi de lloc de treball.

Tots els usuaris han de ser conscients que són responsables de la gestió segura de les seves contrasenyes i han de fer-ne un ús adequat, per això és important la conscienciació i la informació de tot el personal de Cotecom.

Cal restringir l'accés dels usuaris a les xarxes i serveis de xarxa, i a les diferents aplicacions que existeixen a Cotecom, els usuaris no poden tenir els mateixos privilegis ni accedir a tots els sistemes de Cotecom.

Política sobre l'ús de claus i criptografia: Estableix l'ús de controls criptogràfics, amb l'objectiu de protegir la informació d'accessos no autoritzats i la gestió segura de claus.

Política sobre la seguretat física i de l'entorn: Defineix que els recursos de tractament de la informació critica y sensible han d'estar situats en àrees segures i protegides per perímetres de seguretat definits mitjançant barreres de seguretat i controls d'entrada, solen ser necessaris controls especials contra amenaces físiques del CPD (Centre de Processament de Dades), com ara controls antiincendi, de temperatura, SAIs, etc...

Política sobre la gestió d'operacions: Estableix responsabilitats i procediments per la gestió i operació amb els sistemes de la informació. Aquestes gestions i operacions dels sistemes de la informació han de realitzar-se de manera segregada, no tothom pot accedir a tot. D'aquesta manera es redueix el risc de negligència, ús incorrecte o intencionat.

Aquesta política també ha d'establir els mecanismes de protecció necessaris contra el programari maliciós i la definició de la política de copies de seguretat que estableixi la periodicitat de les copies i la seva validació.

També cal establir procediments de revisió i monitorització dels sistemes d'informació, per determinar el seu estat i operativitat en tot moment.

Política sobre la gestió de comunicacions: És fonamental establir una política sobre la gestió de les xarxes ja que a través de la xarxa hi circula tota la informació de Cotecom, tant a nivell intern com a nivell extern.

Cal definir com es realitzarà l'intercanvi d'informació mitjançant contractes i canals segurs, als quals només hi tindrà accés el personal autoritzat.

Política d'adquisició, desenvolupament i manteniment de Sistemes d'Informació: Cal establir els requisits de seguretat en relació al desenvolupament d'aplicacions, adquisició i manteniment de sistemes, cal assegurar que l'aplicació o el sistema funciona correctament, establint proves de seguretat i proves d'acceptació dels sistemes.

Política de gestió de proveïdors: Estableix com cal controlar la seguretat de la informació en relació amb el tracte amb els proveïdors, ha de ser enfocada a les relacions amb els proveïdors, definir els mecanismes per revisar el servei i els canvis en els serveis prestats per els tercers.

Política de gestió d'incidents de seguretat: Cal definir com gestionar les amenaces en seguretat, tot allò que afecti a la seguretat de la informació del negoci, per tant la definició dels incidents vindrà determinat per Cotecom, amb un sistema de gestió d'incidències de seguretat.

Procediment d'Auditories Internes

El Procediment d'auditories internes definirà un pla anual per realitzar les auditories En aquest pla anual es definirà qui realitzarà les auditories, els mètodes que s'utilitzaran, criteris que s'aplicaran, etc. per tal que Cotecom pugui mantenir la certificació vigent.

Objectius de les auditories internes

L'Objectiu de l'auditoria tal com s'ha comentat anteriorment és el de planificar, executar i crear un dels resultats i informes per tal de validar SGSI de l'empresa, per dur el seguiment de la seva política de seguretat.

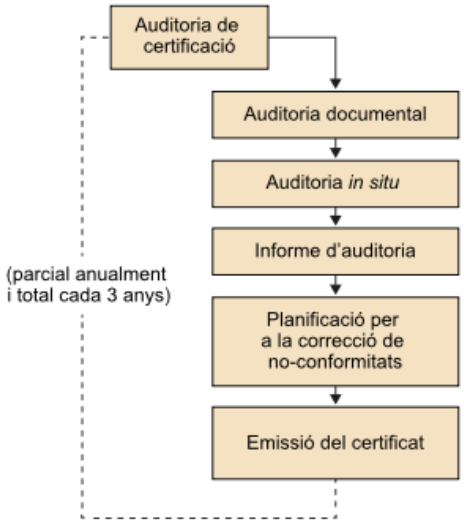
L'auditoria s'encarregarà de validar tot el sistema d'informació de l'empresa i els elements relacionats amb la implantació, correcció i millora d'aquests sistemes d'informació. Controlar les vulnerabilitats detectades, revisar dels controls i indicadors que s'hagin fet servir per la implantació de la norma i la corresponent documentació relativa a la normativa ISO.

Aquesta auditoria s'ha d'executar amb un grup d'auditors interns independents per poder obtenir resultats més objectius. Aquest grup d'auditors interns ha de ser escollit amb el suport de la direcció de l'empresa.

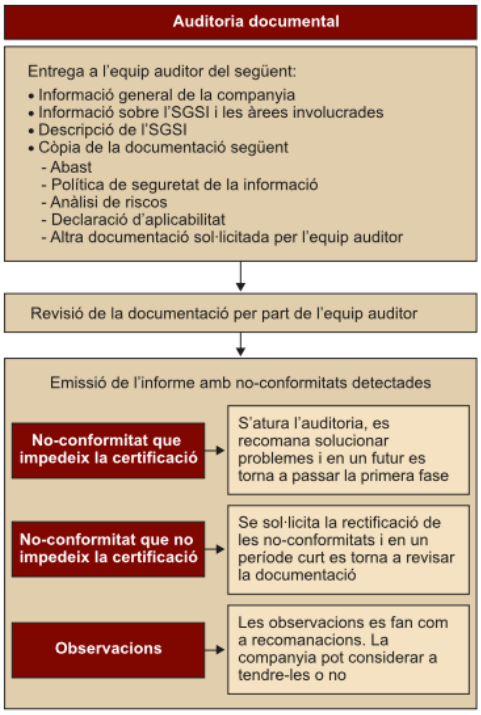
Els controls que es realitzaran a les auditories internes vindran marcats en alguns casos per el compliment legal, per tant aquest procediment inclourà el controls de la LOPD, que realitzaran els auditors interns.

El procediment de l'auditoria

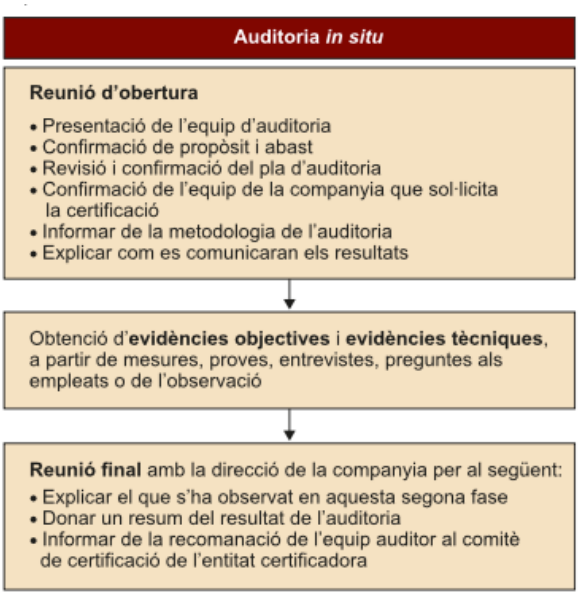
Tal com es diu en els apunts de l'assignatura SGSI (tema 4, punt 6.1 : El procés de certificació) l'auditoria de certificació consta de les següents etapes. Aquestes etapes, exceptuant la d'Emissió del certificat, es poden utilitzar per a realitzar l'auditoria interna:



Auditoria documental: Els auditors revisaran la documentació de SGSI per verificar que Cotecom té la seva documentació actualitzada i en regla.



Auditoria de la certificació: Els auditors verificaran que Cotecom compleix amb les polítiques, objectius i procediments del SGSI i que són correctes, revisió i registre d'incidències, informes de proves de recuperació, procediments i normativa relativa a LOPD...



L'informe de l'auditoria interna serà elaborat per l'equip intern auditor i inclourà:

- La data d'auditoria
- L'equip auditor
- L'abast i la norma de referència
- La conformitat de l'SGSI amb la norma
- Les no conformitats detectades

Finalment, un cop realitzada l'auditoria interna, cal planificar la correcció de les no-conformitats i actualitzar tota la documentació relativa a aquestes.

Gestió d'Indicadors

Per tal que el sistema es mantingui viu i actualitzat, cal avaluar-ne l'eficiència de manera continuada. Per fer-ho s'han d'establir indicadors que permetin controlar el funcionament de les mesures de seguretat de la informació implantades i també l'eficiència que tenen, definint els mecanismes i la periodicitat de mesura d'aquests indicadors.

Un indicador és una mesura respecte d'una referència. Tot indicador consta de vuit components bàsics:

- Nom de l'indicador: Nom breu significatiu que doni idea de quin és el seu ús.
- Descripció de l'indicador: Explicació de l'objectiu de mesura.
- Control de seguretat: A quin control o controls de seguretat dóna cobertura.
- Fórmula de mesurament: Descripció de la formula aplicada per obtenir la mesura.
- Unitats de mesura: Cal que siguin especificades clarament.
- Freqüència de mesura: Cada quant es realitza la mesura.
- Valor objectiu o llindar: Definir quin és el valor correcte o quin és el valor per sota del qual cal aixecar una alarma.
- Responsable de mesura: Sobre qui o quin càrrec recau la responsabilitat de mesurar l'indicador.

Alguns indicadors de gestió:

- Nombre d'hores de formació impartides
- Pressupost dedicat a personal de manteniment de sistemes
- Nombre de suggeriments de millora SGSI rebuts dels treballadors
- Manual de entrada
- Gestió d'altes i baixes o canvis de lloc de treball

Indicadors d'entorn:

- Alertes de virus
- Alerta de temperatura, al centre de processament de dades
- Alerta de d'accés al centre de processament de dades
- Alerta de fallada d'alimentació elèctrica al centre de processament de dades
- Temps de carrega sense alimentació elèctrica dels SAIs
- Estàndards d'autenticació
- Gestió de contrasenyes

Exemple d'indicador

Nom indicador	Alerta de temperatura al centre de processament de dades.
Descripció	Mesura de l'eficiència de l'alerta de temperatura en el centre de processament de dades.
Control de Seguretat	11.1.4
Forma de mesura	Fer pujar la temperatura de la sonda de temperatura interna del CPD
Unitats de mesura	Temperatura
Freqüència de mesura	Cada quatre mesos
Valor Objectiu Valor Llindar	20ºC (temperatura estable) 25ºC (salta alarma)
Responsable de la mesura	Tècnic de sistemes.

Procediments de Revisió per Direcció

Per tal que la implantació de la política de seguretat tingui èxit, cal que la Direcció de l'empresa proporcioni medis i suport per dur a terme els canvis referents a la cultura de la seguretat.

Cal que l'equip de direcció estigui informat de l'estat actual del seu SGSI i de la seva evolució, juntament amb un pla d'acció i inversió en seguretat dels propers anys. D'aquesta manera es podrà ajudar el màxim possible en la pressa de decisions.

Aquest procediment s'executarà un cop l'any un cop finalitzada i valorada l'auditoria interna, i s'entregarà la següent documentació:

- Resultats de l'auditoria interna.
- Informació detallada de l'estat actual del sistema d'informació amb els punt de millora o correcció.
- Pla d'acció amb possibles projectes de millora dels sistemes d'informació.

Amb aquesta informació l'equip de direcció realitzarà el tancament de l'auditoria anual, amb la previsió dels nous objectius pel sistema.

Gestió de Rols i Responsabilitats

En la política de gestió de rols i responsabilitats s'especifica l'equip encarregat de crear, mantenir, supervisar i millorar el sistema d'informació i la seva seguretat basant-se en la ISO 27001:2013. Aquest equip s'anomena comitè de seguretat.

Dintre d'aquesta política s'han definit quatre rols amb les seves responsabilitats:

- Rol usuari: Els treballadors de Cotecom.
- Rol usuari clau: El responsable o usuari clau, que reportarà, supervisarà la informació d'un grup de treballadors al comitè de seguretat, per tal de millorar SGSI
- Rol administració: Personal de Tic que administrarà i gestionarà els permisos.
- Rol responsable seguretat: Persona que coordinarà i supervisarà als usuaris clau i administradors.

Aquests rols formaran part del Comitè de seguretat, representant la seguretat de l'empresa, verificaran el correcte funcionament de la seguretat de l'empresa i aplicació del SGSI, reportant l'estat d'aquesta al responsable de seguretat de Cotecom.

Metodologia d'Anàlisis de Riscos

La Metodologia d'Anàlisis de Riscos marca la sistemàtica que s'haurà de seguir per calcular el risc sobre els actius, amenaces i vulnerabilitats de l'organització. L'anàlisi de risc és un dels punts clau en la implementació, manteniment i millora d'un Sistema de Gestió de la Seguretat de la Informació (SGSI), ja que ens permet identificar els punts febles en nivells de seguretat de la nostra organització.

La metodologia que s'utilitzarà és la Magerit v3[1], una metodologia per l'anàlisi i gestió de riscs en sistemes d'informació elaborada pel Consell Superior d'Administració Electrònica.

Declaració d'Aplicabilitat

La declaració d'aplicabilitat ens indica sobre els diferents controls de la ISO 27001:2013, i ens indica si aplica o no aplica sobre aquests, amb una breu explicació del seu estat actual.

CONTROL				**Aplica?**
A.5 Política de Seguretat de la Informació				
	A.5.1 Directrius de la Direcció en seguretat de la informació			
		A.5.1.1	Conjunt de polítiques per la seguretat de la informació	La direcció ha d'aprovar un document de política de seguretat de la informació, publicar-lo i distribuir-lo a els seus treballadors i tercers afectats.	SI
		A.5.1.2	Revisió de les polítiques per la seguretat de la informació	Cal definir un document de revisió de les polítiques de seguretat, que defineixi els intervals o que hi hagi canvis significatius, aprovat per la direcció.	SI

[1] Es pot trobar més informació de Margerit V3 en el següent enllaç: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=ca#.VGD4lVOG_20

A.6 Organització de la Seguretat de la Informació				
	A.6.1 Organització interna			
		A.6.1.1	Assignació de responsabilitats per la seguretat de la informació	Cal assignar les responsabilitats per a la coordinació dels diferents representats en cada un dels rols.	SI
		A.6.1.2	Segregació de tasques	Cal segregar les tasques per cada un dels rols creat o especialitat.	SI
		A.6.1.3	Contacte amb les autoritats	Cal mantenir el contacte amb les autoritats pertinents perquè tot sigui correcte, en el cas de LOPD.	SI
		A.6.1.4	Contacte amb grups d'interès especial	S'està valorant si val la pena realitzar una auditoria externa o independent de la seguretat de l informació.	NO
		A.6.1.5	Seguretat de la informació en la gestió de projectes	S'han de definir les mesures de seguretat en la gestió de projectes.	SI
	A.6.2 Dispositius mòbils i teletreball				
		A.6.2.1	Política d'us de dispositius mòbils	No hi ha definida una política de dispositius mòbils.	SI
		A.6.2.2	Teletreball	Si existeix una política d'autorització de treball mitjançant VPN, però no global de teletreball.	SI
A.7 Seguretat dels Recursos humans					
	A.7.1 Abans de la contractació				
		A.7.1.1	Investigació d'antecedents	Es realitza una entrevista, anàlisis del candidat, psicotècnic i cerca d'informació relativa a ell.	SI
		A.7.1.2	Termes i condicions de contractació	Es signen clàusules de confidencialitat i de LOPD, però explícitament sobre la seguretat de la informació.	SI
	A.7.2 Durant la contractació				
		A.7.2.1	Gestió de les responsabilitats	Cal explicar i definir les responsabilitats del lloc de treball.	SI
		A.7.2.2	Conscienciació, educació i capacitació en Seg. de la informació	No es realitza cap formació referent a la seguretat de la informació.	SI
		A.7.2.3	Procés disciplinari	No exactament sobre la seguretat informàtica, però si sobre les clàusules de confidencialitat i LOPD, cal actualitzar-ho.	SI
	A.7.3 Cessament o canvi de lloc de treball				
		A.7.3.1	Cessament o canvi de lloc de treball	Si s'assegura la retirada dels drets d'accés dels treballadors i usuaris de terceres parts al seu cessament o canvi de lloc de treball, però no hi ha cap procediment definit.	SI
A.8 Gestió d'actius					
	A.8.1 Responsabilitat sobre els actius				
		A.8.1.1	Inventari d'actius	Existeix i es manté actualitzat l'inventariat dels actius del sistema d'informació, però cal unificar els actius en una mateixa llista.	SI
		A.8.1.2	Propietat dels actius	Estan designats tots els propietaris dels actius, però cal trobar un mètode més correcte.	SI
		A.8.1.3	Us acceptable dels actius	No estan definits i documentades les regles de l'ús acceptable d'actius de sistemes de la	SI

			informació.	
A.8.1.4	Devolució dels actius	S'assegura la devolució de tots els actius de l'organització en possessió dels treballadors i usuaris de terceres parts a la finalització de la contractació, tot i que no existeix cap registre unificat d'actius amb treballadors i usuaris de terceres parts.	SI
A.8.2 Classificació de la informació			
A.8.2.1	Directrius de classificació	No existeix un esquema per classificar la informació i els sistemes en funció de la seva confidencialitat o importància.	SI
A.8.2.2	Etiquetat i manipulat de la informació	No existeixen procediments per identificar i fer servir la informació, en base als esquemes de classificació.	SI
A.8.2.3	Manipulació dels actius	No existeix alguna guia o procediment de manipulació d'actius.	SI
A.8.3 Utilització de suports d'emmagatzematge			
A.8.3.1	Gestió de suports extraïbles	No hi ha procediments per gestionar suports extraïbles amb informació com discs, CD's, informes, impresos...	SI
A.8.3.2	Eliminació de suports	S'han desenvolupat procediments per assegurar el fitxer i la destrucció dels suports informàtics.	SI
A.8.3.3	Suports físics en transit	No es pren cap mesura especial amb els suports en trànsit amb informació sensible.	SI
A.9 Control d'accés			
A.9.1 Requisits del negoci per el control d'accés			
A.9.1.1	Política de control d'accessos	No estan documentades les regles i els drets d'accés dels usuaris i grups.	SI
A.9.1.2	Control d'accés a les xarxes i serveis associats	Existeix un control d'accés a les xarxes i serveis associats.	SI
A.9.2 Gestió d'accés d'usuari			
A.9.2.1	Gestió d'altes/baixes en el registre d'usuaris	Queden registrats els accessos dels usuaris	SI
A.9.2.2	Gestió dels drets d'accés assignats a usuaris	Esta controlada la gestió dels drets d'accés per part TI	SI
A.9.2.3	Gestió dels drets d'accés amb privilegis especials	Està controlada la gestió dels drets d'accés amb privilegis especials per part TI	SI
A.9.2.4	Gestió de informació confidencial d'autenticació d'usuaris.	No es controla la gestió de la informació confidencial referent a l'autenticació dels usuaris, cada usuari és responsable.	NO
A.9.2.5	Revisió dels drets d'accés dels usuaris.	Si es revisen periòdicament els drets d'accés dels usuaris	SI
A.9.2.6	Retirada o adaptació dels drets d'accés	S'assegura la retirada dels drets d'accés dels treballadors i usuaris de terceres parts a la finalització de la contractació o acord.	SI
A.9.3 Responsabilitat dels Usuaris			
A.9.3.1	Ús de la informació confidencial per l'autenticació	No s'explica la responsabilitat de l'ús de la informació confidencial	SI

				per a l'autenticació a els usuaris.	
	A.9.4 Control d'accés a sistemes i aplicacions				
		A.9.4.1	Restricció d'accés a la informació	Esta restringit l'accés a la informació i funcions dels sistemes d'aplicació.	SI
		A.9.4.2	Procediments segurs d'inici de sessió	No existeixen procediments que expliquin com realitzar inicis de sessió segurs.	SI
		A.9.4.3	Gestió de contrasenyes d'usuari	No existeix cap procés per la gestió de contrasenyes.	NO
		A.9.4.4	Us d'eines d'administració de sistemes	S'utilitzen eines pròpies de cada sistema per a l'administració i control dels sistemes informàtics.	SI
		A.9.4.5	Control d'accés al codi font dels programes	Existeix un control d'accés al codi font dels programes	NO
A.10 Criptografia					
	A.10.1 Xifrat				
		A.10.1.1	Política d'us dels controls criptogràfics	No existeix una política que defineixi l'ús de controls de xifrat per la protecció de la informació.	NO
		A.10.1.2	Gestió de contrasenyes	No s'utilitza cap sistema de gestió de les claus per suportar l'ús de les tècniques criptogràfiques.	NO
A.11 Seguretat física i de l'entorn					
	A.11.1 Àrees segures.				
		A.11.1.1	Perímetres de seguretat física.	Existeix un perímetre de seguretat per protegir les àrees on estan els sistemes.	SI
		A.11.1.2	Controls físics d'entrada.	Les àrees estan protegides per controls d'entrada, per permetre l'accés només al personal autoritzat.	SI
		A.11.1.3	Seguretat d'oficines, despatxos i recursos.	Les oficines, despatxos i recursos que tenen algun requeriment de seguretat especial estan protegides amb clau.	NO
		A.11.1.4	Protecció contra les amenaces externes i ambientals.	Les àrees de seguretat estan protegides contra incendis, inundacions, terratrèmols, explosions, disturbis i altres formes de desastres naturals o origen humà.	SI
		A.11.1.5	El treball en àrees segures.	No existeixen controls físics especials per treballar en les àrees segures.	SI
		A.11.1.6	Àrees d'accés públic, carga i descarrega.	Les àrees d'entrada i sortida de mercaderies estan aïllades de l'àrea de sistemes.	SI
	A.11.2 Seguretat dels equips				
		A.11.2.1	Localització i protecció d'equips.	Els equips estan situats o protegits per reduir les opcions d'accés no autoritzat.	SI
		A.11.2.2	Instal·lacions de subministres.	Els equips estan protegits contra fallades de subministrament (llum, aigua, calefacció, aire condicionat, clavegueram)?	SI
		A.11.2.3	Seguretat del cablejat.	El cablejat és segur i compleix amb les normatives industrials vigents.	NO
		A.11.2.4	Manteniment dels equips.	Es mantenen els equips en base a les recomanacions del fabricant i/o	SI

				procediments documentats.	
		A.11.2.5	Sortida d'actius fora de les dependències de l'empresa	No es necessita cap autorització per treure de les oficines equips, informació o software.	SI
		A.11.2.6	Seguretat dels equips i actius fora de les instal·lacions.	No existeixen procediments de seguretat que cobreixin la seguretat dels sistemes quan s'utilitzen fora de les premisses de l'empresa.	NO
		A.11.2.7	Reutilització o retirada segura dels dispositius d'emmagatzematge	Es borra la informació dels equips o dispositius d'emmagatzematge abans de reutilitzar-los o retirar-los.	SI
		A.11.2.8	Equip informàtic d'usuari desatès.	Es sol·licita als usuaris adoptar mesures de protecció amb els equips desatesos.	SI
		A.11.2.9	Política de lloc de treball net i bloqueig de pantalla	No existeix una política de pantalles i lloc de treball net pels entorns de treball.	SI
A.12 Seguretat en les operacions					
	A.12.1 Responsabilitat i procediments d'operació				
		A.12.1.1	Documentació de procediments d'operació.	No estan documentats i mantinguts els procediments operacionals.	SI
		A.12.1.2	Gestió de canvis.	Estan controlats els canvis dels sistemes i aplicacions.	SI
		A.12.1.3	Gestió de capacitats.	No estan gestionades les capacitats, per reduir la oportunitat de mals usos dels sistemes.	SI
		A.12.1.4	Separació d'entorns de desenvolupament, prova i producció.	Estan separades les àrees de desenvolupament i prova de les de els sistemes en operació.	SI
	A.12.2 Protecció contra codi maliciós.				
		A.12.2.1	Controls contra codi maliciós.	Existeixen procediments implantats per protegir a l'empresa contra codi maliciós.	SI
	A.12.3 Copies de seguretat.				
		A.12.3.1	Copies de seguretat de la informació.	Es fan regularment copies de seguretat de la informació per part de TI.	SI
	A.12.4 Registre de l'activitat i supervisió.				
		A.12.4.1	Registre i gestió d'esdeveniments d'activitat.	Existeixen procediments per monitoritzar l'ús de serveis de processos de la informació.	SI
		A.12.4.2	Protecció dels registres d'informació.	No tots els sistemes estan protegits contra manipulació i accés no autoritzat els registres de sistemes de la informació.	SI
		A.12.4.3	Registres d'activitat de l'administrador i operador de sistemes.	No en tots els sistemes es registren i revisen regularment les activitats dels administradors i operador de sistemes.	SI
		A.12.4.4	Sincronització de rellotges.	Estan sincronitzats tots els rellotges dels ordinadors?	SI
	A.12.5 Control del software en explotació				
		A.12.5.1	Instal·lació del software en sistemes en explotació	No s'aplica cap control per implantar software en el sistema en operació.	SI
	A.12.6 Gestió de la vulnerabilitat tècnica.				
		A.12.6.1	Gestió de les vulnerabilitats tècniques.	No es gestionen, analitzen ni corregeixen les vulnerabilitats	SI

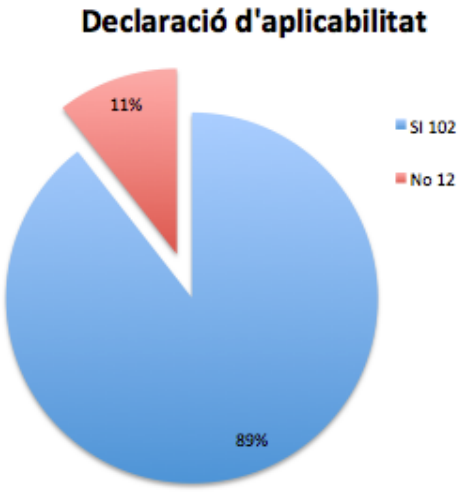
				tècniques de tots els sistemes.	
		A.12.6.2	Restriccions en la instal·lació de software.	No està restringida ni controlada la instal·lació de software.	SI
	A.12.7 Consideracions de les auditories dels sistemes d'informació.				
		A.12.7.1	Controls d'auditoria dels sistemes d'informació.	Només estan planificades les auditories tècniques sobre fallades del sistema.	SI
A.13 Seguretat en les comunicacions					
	A.13.1 Gestió de la seguretat en les xarxes				
		A.13.1.1	Controls de xarxa	Si que s'han implantat algun tipus de control per mantenir la seguretat de la xarxa.	SI
		A.13.1.2	Mecanismes de seguretat associats a els serveis de xarxa.	No estan documentats els atributs de seguretat de tots els serveis de xarxa.	SI
		A.13.1.3	Segregació de Xarxes	Existeix una segregació de xarxes segons les necessitats de cada una.	SI
	A.13.2 Intercanvi d'informació amb parts externes.				
		A.13.2.1	Polítiques i procediments d'intercanvi d'informació.	No estan documentades les polítiques, procediment i mesures per intercanvi d'informació a través de tots els tipus formes de comunicació.	SI
		A.13.2.2	Acords d'intercanvi.	No s'han establert acords amb altres empreses per intercanviar informació o aplicacions.	SI
		A.13.2.3	Missatgeria electrònica.	El comerç electrònic no està protegit contra activitats fraudulentes.	SI
		A.13.2.4	Acords de confidencialitat i secret	Si que es firmen acords de confidencialitat amb intercanvi d'informació amb parts externes.	SI
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.					
	A.14.1 Requisits de seguretat dels sistemes d'informació.				
		A.14.1.1	Anàlisis i especificacions dels requisits de seguretat.	No s'han especificat els controls de seguretat necessaris per nous sistemes o millores dels actuals.	SI
		A.14.1.2	Seguretat en les comunicacions en serveis accessibles per xarxes publiques.	Si que estan assegurades les comunicacions a serveis quan s'accedeix des de xarxes publiques.	Si
		A.14.1.3	Protecció de les transaccions per xarxes de comunicacions.	S'estableix protecció en les transaccions que es realitzen mitjançant xarxes de comunicacions, segons els requeriments del destinatari.	SI
	A.14.2 Seguretat ens els processos de desenvolupament i suport				
		A.14.2.1	Polítiques de desenvolupament segur de software.	No s'ha establert una política de desenvolupament segur de software.	NO
		A.14.2.2	Procediments de control de canvis en els sistemes.	No existeix un procediment de control de canvis o versions en els sistemes o programes informàtics.	SI
		A.14.2.3	Revisió tècnica de les aplicacions després de fer canvis en el SO.	No es realitza una revisió tècnica després de realitzar canvis.	SI
		A.14.2.4	Restriccions en els canvis en els paquets de software.	No hi ha una política de restriccions en els canvis en els paquets de software	SI

	A.14.2.5	Us de principis d'enginyeria en protecció de sistemes.	No s'utilitzen principis d'enginyeria en la protecció de sistemes.	NO
	A.14.2.6	Seguretat en entorns de desenvolupament	Si s'utilitzen mètodes de seguretat en l'accés a entorns de desenvolupament.	SI
	A.14.2.7	Externalització del desenvolupament de software	No està procedimentat, controlat i verificat l'externalització del desenvolupament de software.	SI
	A.14.2.8	Proves de funcionalitat durant el desenvolupament de sistemes	No es realitzen proves de funcionalitat durant els desenvolupament de sistemes	SI
	A.14.2.9	Proves d'acceptació.	Si que es realitzen proves d'acceptació dels desenvolupaments en els entorns de desenvolupament o test	SI
A.14.3 Prova de dades				
	A.14.3.1	Protecció de les dades utilitzades en proves.	Si que es protegeixen les dades utilitzades en les proves.	SI
A.15 Relació amb els proveïdors				
A.15.1 Seguretat de la informació en les relacions amb proveïdors.				
	A.15.1.1	Política de seguretat de la informació per proveïdors.	No s'ha establert una política de la seguretat de la informació per a proveïdors.	SI
	A.15.1.2	Tractament del risc dintre d'acords de proveïdors.	No existeix un document que tracti el risc dintre dels acords de proveïdors de sistemes informàtics.	SI
	A.15.1.3	Cadena de subministrament en tecnologies de la informació i comunicacions.	No està controlada la cadena de subministrament en tecnologies de la informació i comunicació.	NO
A.15.2 Gestió de la prestació del servei per proveïdors.				
	A.15.2.1	Supervisió i revisió dels serveis prestats per tercers.	Si que es realitza una supervisió dels serveis prestats per tercers.	SI
	A.15.2.2	Gestió de canvis en els serveis prestats per tercers.	Si que existeix una gestió de canvis en els serveis prestats per tercer.	SI
A.16 Gestió de incidències de seguretat de la informació				
A.16.1 Gestió de incidències de seguretat de la informació				
	A.16.1.1	Responsabilitats i procediments.	No s'han establert procediments i responsabilitats per la gestió d'incidents.	SI
	A.16.1.2	Notificació dels esdeveniments de seguretat de la informació.	No existeix un canal a través del qual es reportin els incidents de seguretat.	SI
	A.16.1.3	Notificació dels punts dèbils de la seguretat.	No es sol·licita als usuaris que comuniquin qualsevol debilitat de seguretat o amenaça pel sistema.	SI
	A.16.1.4	Valoració dels esdeveniments de seguretat de la informació i pressa de decisions.	Si que es valoren i es pren una decisió sobre els esdeveniments de seguretat de la informació, però no està procedimentat.	SI
	A.16.1.5	Resposta a els incidents de seguretat.	Si que es corregeixen els incidents de seguretat.	SI
	A.16.1.6	Aprenentatge dels incidents de seguretat informàtica.	No tenim mecanismes funcionant per realitzar anàlisis del tipus volum i cost de les incidències i errades?	SI
	A.16.1.7	Recopilació d'evidències.	No es mantenen les evidencies, conforme a les lleis i normes publicades, per recolzar una acció contra una persona o organització.	SI

A.17 Els aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci.				
	A.17.1 Continuïtat de la seguretat de la informació			
		A.17.1.1	Planificació de la continuïtat de la seguretat de la informació.	No existeix un pla estratègic basat en la valoració de risc, on es detallin les accions per la continuïtat del negoci.	SI
		A.17.1.2	Implantació de la continuïtat de la seguretat de la informació.	Els plans de continuïtat per mantenir o restaurar les operacions del negoci en un temps raonable no estan desenvolupats.	SI
		A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	No es verifiquen, revisen i avaluen regularment els plans de continuïtat de negoci per assegurar que són eficaços.	SI
	A.17.2 Redundàncies				
		A.17.2.1	Disponibilitat d'instal·lacions per el processament de la informació.	Si que existeixen redundàncies en la disponibilitat d'instal·lacions per al processament de la informació, que permetin suportar talls energia elèctrica, aigua, comunicacions...	SI
A.18 Compliment				
	A.18.1 Compliment dels requeriments legals i contractuals.			
		A.18.1.1	Identificació de la legislació aplicable.	No estan definits i documentats, per cada sistema d'informació, tots els requeriments contractuals, reguladors i estatutaris.	SI
		A.18.1.2	Drets de propietat intel·lectual (DPI).	No hi ha procediments per assegurar el compliment amb les restriccions legals en l'ús de material referent als drets de la propietat intel·lectual.	SI
		A.18.1.3	Protecció dels registres de l'organització.	Si estan protegits contra pèrdua, destrucció i falsificació els registres importants, en cada servei.	SI
		A.18.1.4	Protecció de dades i privacitat de la informació personal.	Si existeixen controls eficaços per protegir la informació personal en base a la legislació vigent, la LOPD	SI
		A.18.1.5	Regulació dels controls criptogràfics.	No existeixen controls per assegurar el compliment amb els acords nacionals per controlar l'ús de xifrat.	SI
	A.18.2 Revisions de la seguretat de la informació.				
		A.18.2.1	Revisió independent de la seguretat de la informació.	No existeix algun control/auditoria independent/externa de la seguretat de la informació.	SI
		A.18.2.2	Compliment de les polítiques i normes de seguretat.	La direcció no assegura que s'estan seguint correctament els procediments de seguretat, dintre de la seva àrea de responsabilitat.	SI
		A.18.2.3	Comprovació del compliment.	No es revisen regularment els sistemes d'informació per verificar el compliment amb els estàndards d'implantació de seguretat.	SI

Valoració d'Aplicabilitat

Després de realitzar la declaració d'aplicabilitat podem veure que dels 114 controls de la Norma ISO 27001:2013, 12 no són aplicables a Cotecom, per tant 102 si que ho son.



D'aquesta manera, podem dir que haurem d'aplicar 102 controls, dels quals 39 ja es realitzen, però que caldrà revisar, per tal d'estar dins de la Norma ISO 27001:2013.

Anàlisis de riscos

Introducció

No podem protegir tot allò que no coneixem. Es per això, que la primera etapa cap a al Pla d'Implantació d'un SGSI consisteix en la avaluació dels nostres actius, considerant les dependències existents entre ells i fent la valoració dels mateixos.

L'elaboració d'una metodologia d'anàlisis de riscos: Identificació i valoració dels actius, amenaces, vulnerabilitats, càlculs del risc, nivell de risc acceptable i risc residual.

A continuació s'exposa el resultat de l'estudi d'anàlisis de risc del SGSI realitzat als sistemes d'informació de Cotecom.

Inventari d'actius

L'estudi dels actius vinculats a la informació és el primer punt per a l'anàlisi de riscos, per tal de fer-ho utilitzarem la metodologia MARGERIT, entenent com a actiu segons MARGERIT: Els recursos del sistema de informació o relacionats amb aquest, necessaris per a que la organització funcioni correctament i assoleixi els objectius proposats per la seva direcció. També es pot definir actiu com a béns de l'organització o empresa, relacionats amb l'activitat de l'empresa. La metodologia MARGERIT agrupa aquests actius en els següents grups:

- Instal·lacions
- Hardware
- Aplicació
- Dades
- Xarxa
- Serveis
- Equipament Auxiliar
- Personal

Llistat d'actius

Àmbit	ID	Actiu
Instal·lacions	I1	CPD - Centre Procés de Dades
	I2	Sala Comunicacions
	I3	Sala Generador Elèctric
	I4	Armaris de Xarxa
	I5	Resta de sales

Àmbit	ID	Actiu
Hardware	H1	Vir1 IBM x3550 M3 (Entorn ESX VSphere 5.5U1)
	H2	Vir2 IBM x3550 M3
	H3	Vir3 IBM x3550 M3
	H4	Vir4 IBM x3650 M4
	H5	Sun T4 (Servidor SAPP)
	H6	Sunfire v240 (Servidor SAPD)
	H8	Consola control
	H9	Servidor de Backup
	H10	Cabina dades històric
	H11	Cabina de dades IBM DS3512
	H12	Cabina de dades IBM V3700
	H13	Cabina Sap Disc
	H14	Equips oficina sobre taules
	H15	Equips oficina portàtils
	H16	Equips oficina portàtils direcció
	H17	Smartphones
	H18	Antenes Wifi
	H19	Controladora Wifi
	H20	Electrònica de xarxa Cisco
	H21	Firewall Fortinet
	H22	Centres de copiat
	H23	Projectors del les sales de reunions
	H24	Robot Cintes

Àmbit	ID	Actiu
Aplicació	A1	Sistemes operatius servidors: - Microsoft Windows server 2012 - Linux Red Hat 6 i 7 - Sun Solaris 10
	A2	Microsoft Windows 7 i 8 (sistemes operatiu personal)
	A3	Android, IOS i Blackberry (sistemes operatius smartphones)
	A4	Gestor documental Alfresco
	A5	Antivirus Eset Nod32
	A6	Sistema de Backup
	A10	Sistema ERP SAP
	A11	Entorn de disseny PLM – Windchill
	A12	Repositori de fitxers samba
	A13	Correu Google Apps

	A14	Ofimàtica Office Professional 2010 i 2013

Àmbit	ID	Actiu
Dades	D1	Base de dades SAP
	D2	Base de dades PLM
	D3	Base de dades Alfresco

Àmbit	ID	Actiu
Xarxes	X1	Xarxa interna fibra òptica
	X2	Xarxa LAN Cable
	X3	Xarxa WLAN
	X4	Xarxa telefonia mòbil
	X5	Servei internet primari fibra òptica 300/300
	X6	Servei internet backup fibra òptica 10/10
	X7	Telefonia Fixa
	X8	Xarxa Elèctrica

Àmbit	ID	Actiu
Serveis	S1	A5 Nomina - RRHH
	S3	Correu electrònic i missatgeria Google Apps
	S4	Servei de fitxers Samba
	S5	Servei gestor documental Alfresco
	S6	Servei ERP SAP
	S7	Servei gestor de projectes i producte PLM – Windchill

Àmbit	ID	Actiu
Equipament auxiliar	EA1	Aires condicionats STULZ CPD
	EA2	Sistemes SAI Riello CPD
	EA3	Sistema antincendi
	EA4	Sistema control temperatura, humitat.
	EA6	Generador

Àmbit	ID	Actiu
Personal	P1	Director General
	P2	Director Serveis Corporatius (Finances, RRHH, IT i Jurídic)
	P3	Director Comercial
	P4	Director Industrial
	P5	Director Tècnic
	P6	Director de Compres
	P7	Responsable Qualitat, Salut i Medi Ambient
	P8	Responsable TIC
	P9	Responsable Planificació
	P10	Responsable R+D+I
	P11	Responsable Enginyeria
	P12	Responsable Finances
	P13	Responsable RRHH
	P14	Administració Comptabilitat i finances
	P15	Comercials

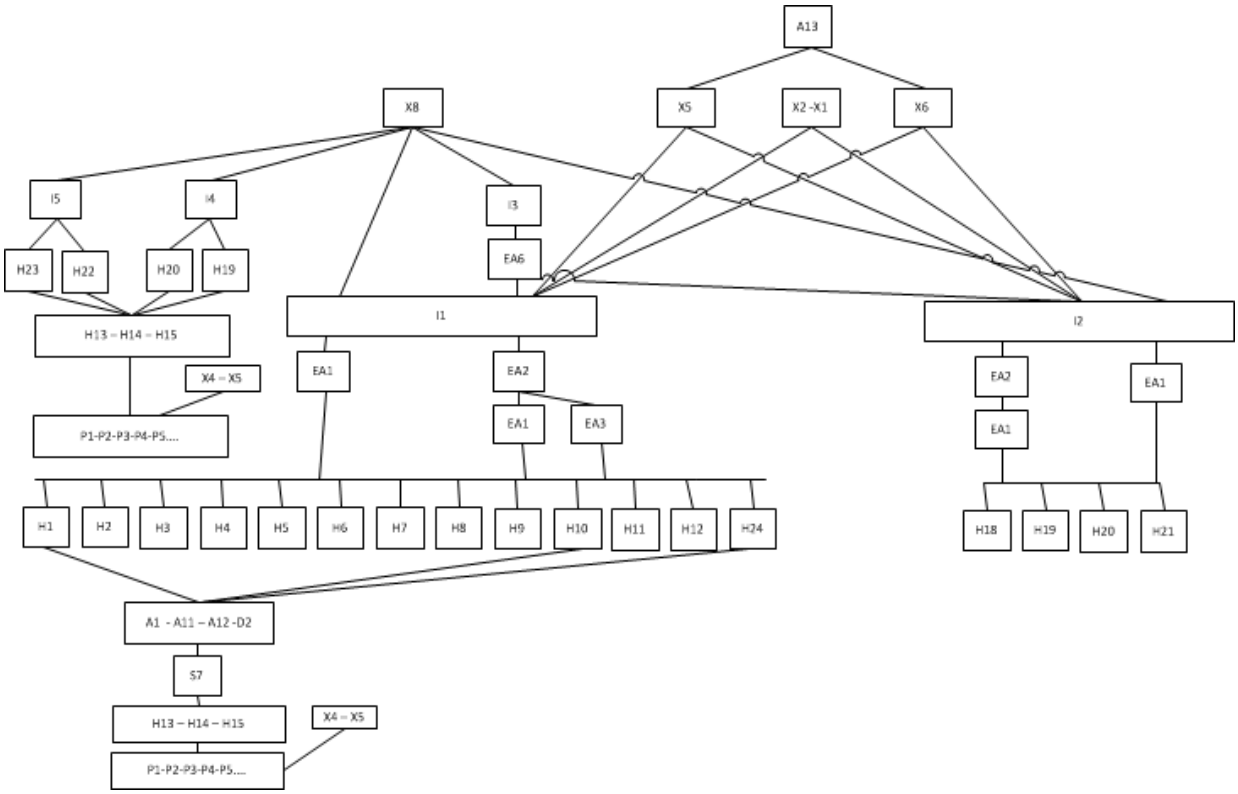
	P16	Administradors TIC
	P17	RRHH
	P18	Enginyeria
	P19	Personal recepció
	P20	Muntatge
	P21	Compres
	P22	Logística

Dependència d'actius

La segona etapa de l'anàlisi de risc dintre de la gestió d'actius consisteix en establir les dependències entre els diferents actius d'una manera jeràrquica, avaluant el grau de vinculació entre equips i en funció dels paràmetres disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat (DICAT).

La dependència entre actius fa que en el cas que una amenaça afecti a un actiu del que depengui un altre actiu superior, tindrà impacte directe sobre l'actiu superior. Per portar a terme la definició de dependències es poden fer preguntes del tipus: qui depèn de qui? Si hi ha una errada en l'actiu X quins altres actius es veuran perjudicats o involucrats?
El resultat d'aquest anàlisis serà un arbre de dependències d'actius en el que es podrà veure la relació existent.

A continuació, es pot veure com seria aquest arbre de dependències d'actius. En aquest exemple es veu com seria l'arbre de dependències fins al servei final. En aquest cas S7 Servei gestió de projectes i producte PLM – Windchill.



Valoració d'actius

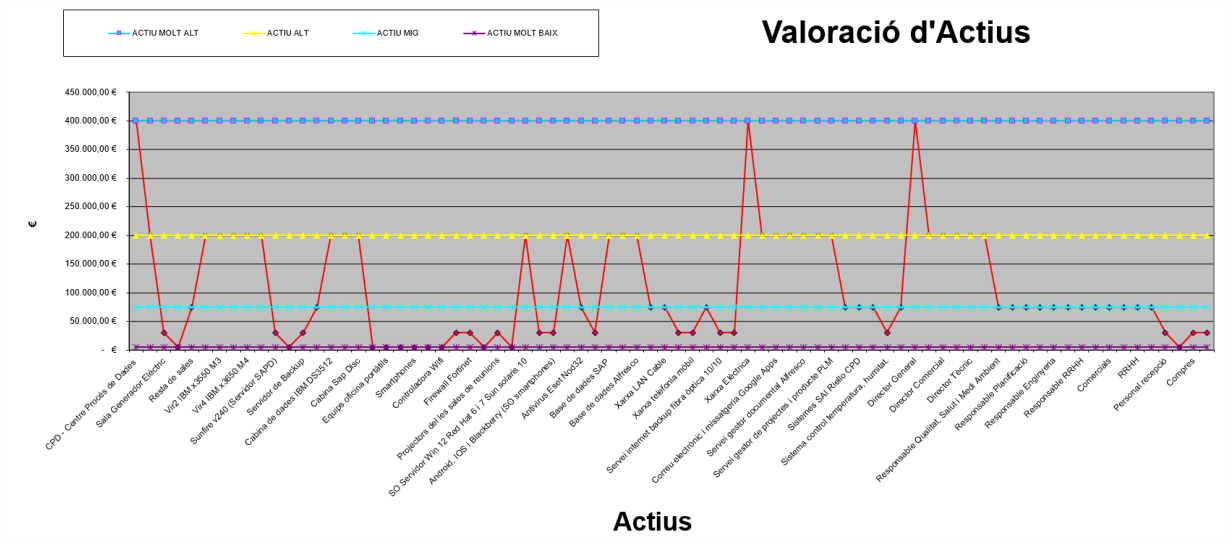
La valoració d'actius consisteix segons MAGERIT en realitzar una estimació quantitativa de cada actiu, tenint en compte paràmetres com podrien ser el cost de la seva reposició, l'ús, la repercussió que pot tenir la seva avaria o caiguda de servei o el temps de reposar l'actiu. Un cop obtinguts els paràmetres es podrà realitzar la valoració sobre 5 nivells, tal com es veu a continuació.

Valoració	ID	Valor
Molt Alt	MA	400.000€
Alt	A	200.000€
Mitja	M	75.000€
Baix	B	30.000€
Molt Baixa	MB	5.000€

Nº	Codi	Descripció	Valoració Quantitativa	Valoració Qualitativa
1	I1	CPD - Centre Procés de Dades	400.000,00 €	MA
2	I2	Sala Comunicacions	200.000,00 €	A
3	I3	Sala Generador Elèctric	30.000,00 €	B
4	I4	Armaris de Xarxa	5.000,00 €	MB
5	I5	Resta de sales	75.000,00 €	M
6	H1	Vir1 IBM x3550 M3 (Entorn ESX VSphere 5.5U1)	200.000,00 €	A
7	H2	Vir2 IBM x3550 M3	200.000,00 €	A
8	H3	Vir3 IBM x3550 M3	200.000,00 €	A
9	H4	Vir4 IBM x3650 M4	200.000,00 €	A
10	H5	Sun T4 (Servidor SAPP)	200.000,00 €	A
11	H6	Sunfire v240 (Servidor SAPD)	30.000,00 €	B
12	H7	Consola control	5.000,00 €	MB
13	H8	Servidor de Backup	30.000,00 €	B
14	H9	Cabina dades històric	75.000,00 €	M
15	H10	Cabina de dades IBM DS3512	200.000,00 €	A
16	H11	Cabina de dades IBM V3700	200.000,00 €	A
17	H12	Cabina Sap Disc	200.000,00 €	A
18	H13	Equips oficina sobre taules	5.000,00 €	MB
19	H14	Equips oficina portàtils	5.000,00 €	MB
20	H15	Equips oficina portàtils direcció	5.000,00 €	MB
21	H16	Smartphones	5.000,00 €	MB
22	H17	Antenes Wifi	5.000,00 €	MB
23	H18	Controladora Wifi	5.000,00 €	MB
24	H19	Electrònica de xarxa Cisco	30.000,00 €	B
25	H20	Firewall Fortinet	30.000,00 €	B
26	H21	Centres de copiat	5.000,00 €	MB
27	H22	Projectors del les sales de reunions	30.000,00 €	B
28	H23	Robot Cintes	5.000,00 €	MB
29	A1	SO Servidor Win 12 Red Hat 6 i 7 Sun solaris 10	200.000,00 €	A
30	A2	Microsoft Windows 7 i 8 SO Personal	30.000,00 €	B
31	A3	Android, IOS i Blackberry (SO smartphones)	30.000,00 €	B
32	A4	Gestor documental Alfresco	200.000,00 €	A
33	A5	Antivirus Eset Nod32	75.000,00 €	M
34	A6	Sistema de Backup	30.000,00 €	B
35	D1	Base de dades SAP	200.000,00 €	A

36	D2	Base de dades PLM	200.000,00 €	A
37	D3	Base de dades Alfresco	200.000,00 €	A
38	X1	Xarxa interna fibra òptica	75.000,00 €	M
39	X2	Xarxa LAN Cable	75.000,00 €	M
40	X3	Xarxa WLAN	30.000,00 €	B
41	X4	Xarxa telefonia mòbil	30.000,00 €	B
42	X5	Servei internet primari fibra òptica 300/300	75.000,00 €	M
43	X6	Servei internet backup fibra òptica 10/10	30.000,00 €	B
44	X7	Telefonia Fixa	30.000,00 €	B
45	X8	Xarxa Elèctrica	400.000,00 €	MA
46	S1	A5 Nomina - RRHH	200.000,00 €	A
47	S3	Correu electrònic i missatgeria Google Apps	200.000,00 €	A
48	S4	Servei de fitxers Samba	200.000,00 €	A
49	S5	Servei gestor documental Alfresco	200.000,00 €	A
50	S6	Servei ERP SAP	200.000,00 €	A
51	S7	Servei gestor de projectes i producte PLM	200.000,00 €	A
52	EA1	Aires condicionats STULZ CPD	75.000,00 €	M
53	EA2	Sistemes SAI Riello CPD	75.000,00 €	M
54	EA3	Sistema antincendi	75.000,00 €	M
55	EA4	Sistema control temperatura, humitat.	30.000,00 €	B
56	EA6	Generador	75.000,00 €	M
57	P1	Director General	400.000,00 €	MA
58	P2	Director Serveis Corp. (Fin., RRHH, IT i Jurídic)	200.000,00 €	A
59	P3	Director Comercial	200.000,00 €	A
60	P4	Director Industrial	200.000,00 €	A
61	P5	Director Tècnic	200.000,00 €	A
62	P6	Director de Compres	200.000,00 €	A
63	P7	Responsable Qualitat, Salut i Medi Ambient	75.000,00 €	M
64	P8	Responsable TIC	75.000,00 €	M
65	P9	Responsable Planificació	75.000,00 €	M
66	P10	Responsable R+D+I	75.000,00 €	M
67	P11	Responsable Enginyeria	75.000,00 €	M
68	P12	Responsable Finances	75.000,00 €	M
69	P13	Responsable RRHH	75.000,00 €	M
70	P14	Administració Comptabilitat i finances	75.000,00 €	M
71	P15	Comercials	75.000,00 €	M
72	P16	Administradors TIC	75.000,00 €	M
73	P17	RRHH	75.000,00 €	M
74	P18	Enginyeria	75.000,00 €	M
75	P19	Personal recepció	30.000,00 €	B
76	P20	Muntatge	5.000,00 €	MB
77	P21	Compres	30.000,00 €	B
78	P22	Logística	30.000,00 €	B

En el següent gràfic es pot veure una visió global dels actius i el seu valor.



Dimensions de seguretat

Un cop identificats els actius, cal valorar-los segons el seu impacte en les cinc dimensions de la seguretat informàtica, autenticitat, confidencialitat, integritat, disponibilitat i traçabilitat, altrament dit per les seves sigles ACIDT. Això ens permetrà valorar l'impacte d'una amenaça sobre l'actiu exposat.

ID	Nom	Definició
A	Autenticitat i no-repudi	Permet assegurar la identitat dels recursos, documents, usuaris o processos del sistema d'informació
C	Confidencialitat	Permet assegurar que només els usuaris autoritzats poden tenir accés a la informació dels diferents nivells de seguretat
I	Integritat	Permet assegurar que la informació és completa i exacta, i que no ha estat manipulada per usuaris no autoritzats
D	Disponibilitat	Permet assegurar que la informació, els sistemes i els processos, estaran disponibles pels usuaris autoritzats en el moment que sigui necessari.
T	Traçabilitat	Permet seguir el recorregut històric d'un procés, document o informació concreta, determinant precisament quin usuari ha realitzat cadascuna de les accions.

El valor que rebi un actiu pot ser propi o acumulat. El valor propi s'assignarà a la informació, quedant la resta d'actius subordinats a les necessitats d'explotació i protecció de la informació. D'aquesta manera, els actius inferiors en un esquema de dependències acumulen el valor dels actius que es recolzen en ells. Cada actiu de informació pot tenir un valor diferent a cadascuna de les diferents dimensions per a la organització que desitgem analitzar.

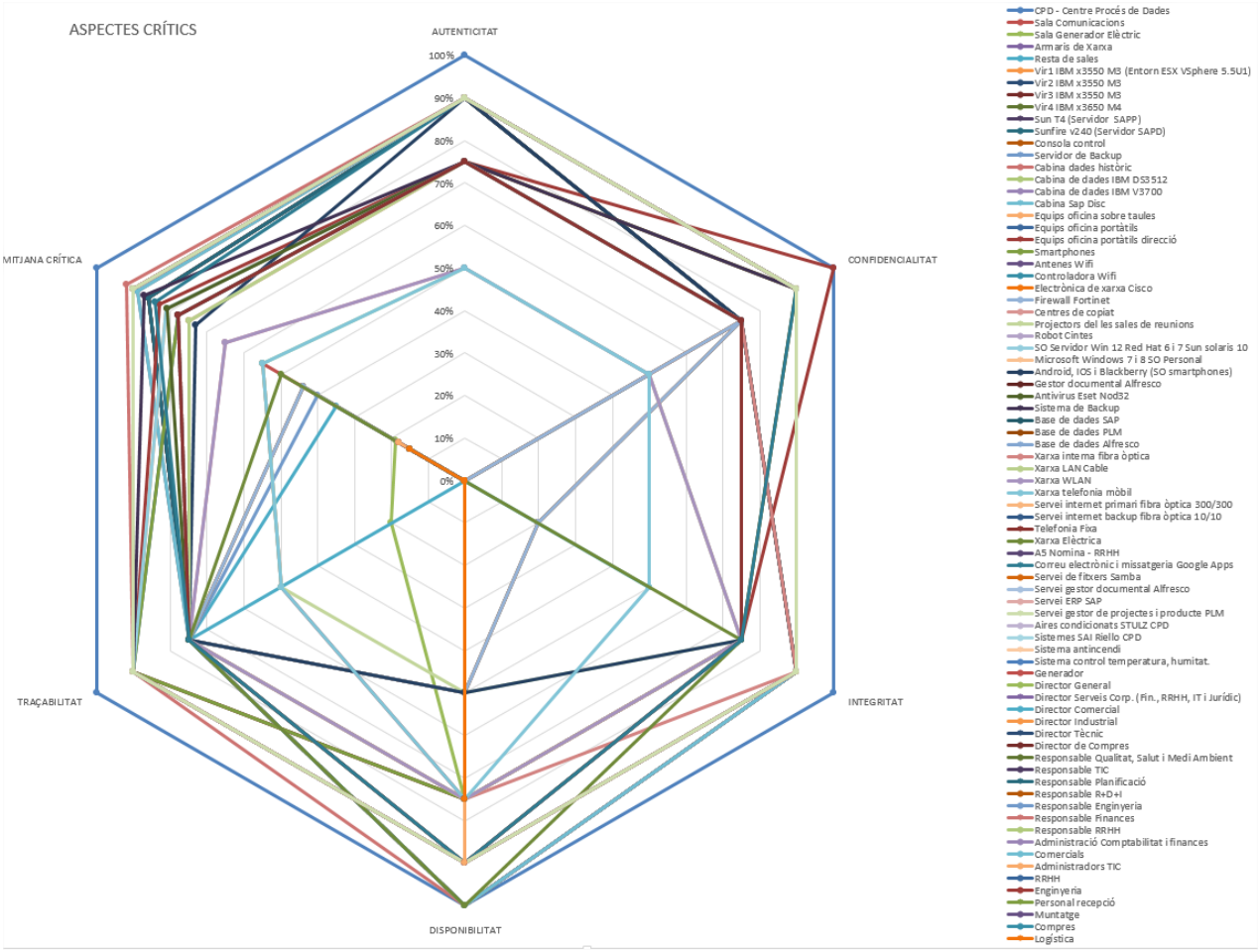
Impacte sobre els actius de ACIDT

Valor	Impacte	ID	Definició
100%	Molt Crític	MC	Dany molt greu
90%	Crític	C	Dany greu a l'organització
75%	Alt	A	Dany molt important a la organització
50%	Mig	M	Dany important a la organització
20%	Baix	B	Dany menor a la organització
0%	No apreciable	N	No afecten a la organització

		Aspectes Crítics					
ID	ACTIU	AUTENTICITAT	CONFIDENCIALITAT	INTEGRITAT	DISPONIBILITAT	TRAÇABILITAT	MITJANA CRÍTICA
I1	CPD - Centre Procés de Dades	100%	100%	100%	100%	100%	100%
I2	Sala Comunicacions	0	75%	75%	75%	50%	55%
I3	Sala Generador Elèctric	0	0	0	75%	20%	19%
I4	Armaris de Xarxa	0	0	0	75%	0	15%
I5	Resta de sales	0	50%	50%	0	75%	35%
H1	Vir1 IBM x3550 M3 (Entorn ESX VSphere 5.5U1)	90%	75%	90%	100%	75%	86%
H2	Vir2 IBM x3550 M3	90%	75%	90%	100%	75%	86%
H3	Vir3 IBM x3550 M3	90%	75%	90%	100%	75%	86%
H4	Vir4 IBM x3650 M4	90%	75%	90%	100%	75%	86%
H5	Sun T4 (Servidor SAPP)	90%	75%	90%	100%	75%	86%
H6	Sunfire v240 (Servidor SAPD)	90%	75%	90%	100%	75%	86%
H8	Consola control	-	-	-	-	-	0%
H9	Servidor de Backup	-	50%	-	75%	75%	40%
H10	Cabina dades històric	90%	90%	90%	100%	90%	92%
H11	Cabina de dades IBM DS3512	90%	90%	90%	100%	75%	89%
H12	Cabina de dades IBM V3700	90%	90%	90%	100%	75%	89%
H13	Cabina Sap Disc	90%	90%	90%	100%	75%	89%
H14	Equips oficina sobre taules	75%	90%	75%	75%	90%	81%
H15	Equips oficina portàtils	75%	75%	75%	75%	90%	78%
H16	Equips oficina portàtils direcció	75%	100%	75%	75%	90%	83%
H17	Smartphones	75%	75%	75%	75%	90%	78%
H18	Antenes Wifi	-	75%	20%	50%	75%	44%
H19	Controladora Wifi	-	75%	20%	50%	75%	44%
H20	Electrònica de xarxa Cisco	-	75%	20%	50%	75%	44%
H21	Firewall Fortinet	-	75%	20%	50%	75%	44%
H22	Centres de copiat	50%	50%	75%	75%	75%	65%

H23	Projectors del les sales de reunions	50%	50%	75%	50%	50%	55%
H24	Robot Cintes	75%	75%	75%	75%	75%	75%
A1	SO Servidor Win 12 Red Hat 6 i 7 Sun solaris 10	75%	75%	75%	90%	90%	81%
A2	Microsoft Windows 7 i 8 SO Personal	75%	75%	75%	75%	75%	75%
A3	Android, IOS i Blackberry (SO smartphones)	90%	75%	75%	50%	75%	73%
A4	Gestor documental Alfresco	90%	90%	90%	90%	90%	90%
A5	Antivirus Eset Nod32	75%	90%	75%	90%	75%	81%
A6	Sistema de Backup	75%	90%	90%	90%	90%	87%
D1	Base de dades SAP	90%	90%	90%	90%	90%	90%
D2	Base de dades PLM	90%	90%	90%	90%	90%	90%
D3	Base de dades Alfresco	90%	90%	90%	90%	90%	90%
X1	Xarxa interna fibra òptica	75%	75%	90%	75%	75%	78%
X2	Xarxa LAN Cable	75%	75%	75%	75%	75%	75%
X3	Xarxa WLAN	50%	50%	75%	75%	75%	65%
X4	Xarxa telefonia mòbil	50%	50%	50%	75%	50%	55%
X5	Servei internet primari fibra òptica 300/300	75%	75%	75%	90%	75%	78%
X6	Servei internet backup fibra òptica 10/10	75%	75%	75%	90%	75%	78%
X7	Telefonia Fixa	75%	75%	75%	90%	75%	78%
X8	Xarxa Elèctrica	-	-	75%	100%	75%	50%
S1	A5 Nomina - RRHH	90%	90%	90%	90%	90%	90%
S3	Correu electrònic i missatgeria Google Apps	90%	90%	75%	90%	75%	84%
S4	Servei de fitxers Samba	90%	90%	90%	90%	90%	90%
S5	Servei gestor documental Alfresco	90%	90%	90%	90%	90%	90%
S6	Servei ERP SAP	90%	90%	90%	90%	90%	90%
S7	Servei gestor de projectes i producte PLM	90%	90%	90%	90%	90%	90%
EA1	Aires condicionats STULZ CPD	-	-	-	90%	-	18%
EA2	Sistemes SAI Riello CPD	-	-	-	90%	-	18%
EA3	Sistema antincendi	-	-	-	90%	-	18%
EA4	Sistema control temperatura, humitat.	-	-	-	90%	-	18%
EA6	Generador	-	-	-	90%	-	18%
P1	Director General	0	0	0	75%	0	15%
P2	Director Serveis Corp. (Fin., RRHH, IT i Jurídic)	0	0	0	75%	0	15%
P3	Director Comercial	0	0	0	75%	0	15%
P4	Director Industrial	0	0	0	75%	0	15%
P5	Director Tècnic	0	0	0	75%	0	15%
P6	Director de Compres	0	0	0	75%	0	15%
P7	Responsable Qualitat, Salut i Medi Ambient	0	0	0	75%	0	15%
P8	Responsable TIC	0	0	0	90%	0	18%
P9	Responsable Planificació	0	0	0	75%	0	15%
P10	Responsable R+D+I	0	0	0	75%	0	15%
P11	Responsable Enginyeria	0	0	0	75%	0	15%

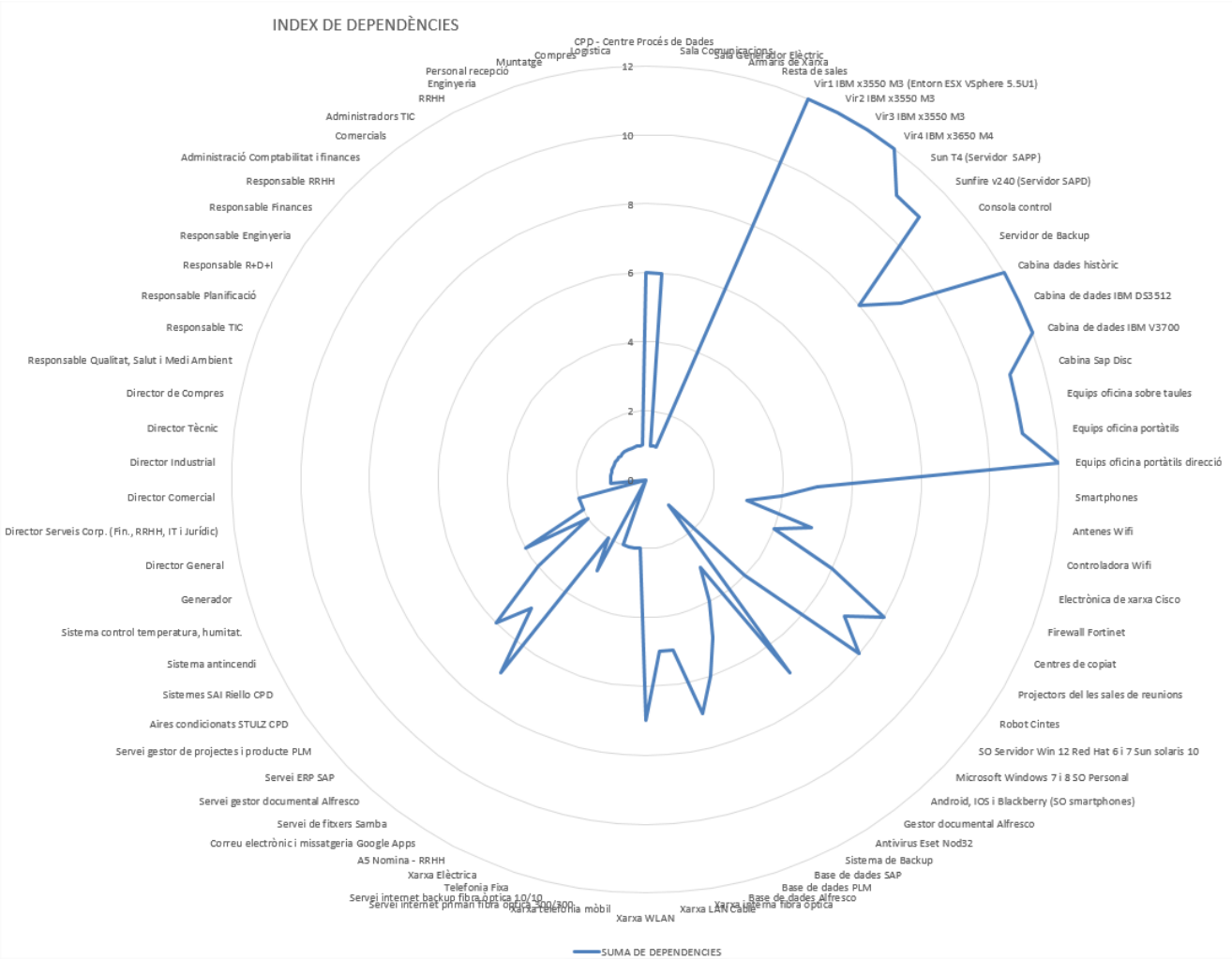
P12	Responsable Finances	0	0	0	75%	0	15%
P13	Responsable RRHH	0	0	0	75%	0	15%
P14	Administració Comptabilitat i finances	0	0	0	75%	0	15%
P15	Comercials	0	0	0	75%	0	15%
P16	Administradors TIC	0	0	0	90%	0	18%
P17	RRHH	0	0	0	75%	0	15%
P18	Enginyeria	0	0	0	75%	0	15%
P19	Personal recepció	0	0	0	75%	0	15%
P20	Muntatge	0	0	0	75%	0	15%
P21	Compres	0	0	0	75%	0	15%
P22	Logística	0	0	0	75%	0	15%



En la taula anterior tenim els diferents actius amb la seva mitjana de criticitat i índex de dependència, la mitjana de criticitat va de 100% com a valor màxim (actiu més crític) a 0 com a valor mínim (actiu menys crític). Per altre banda també tenim l'índex de dependència per categories que va del màxim de dependència 7 al mínim 0.

També en el gràfic anterior es veu de manera resumida ACIDT de cada actiu juntament amb la seva mitjana crítica.

En el següent gràfic es poden veure les dependències de cada actiu respecte els altres actius. Per exemple, el CPD té 6 dependències, Xarxa elèctrica, Aires condicionats, Sistemes SAI, Sistema antiincendi, Sistema control de temperatura i humitat i Generador.



Anàlisis d'amenaces

En l'anàlisi d'amenaces cal estudiar com els actius estan exposats a amenaces i com aquestes poden afectar els diferents aspectes de la seguretat.

En aquest cas, tal com comenta l'anunciat, s'utilitzaran les utilitzades en la metodologia MARGERIT, per un tema d'homogeneïtat, llavors les amenaces es troben classificades en els següents blocs:

- Desastres naturals
- D'origen industrial
- Errors i fallides no intencionats
- Atacs intencionats

Per poder determinar la freqüència amb la que es pot materialitzar una amenaça, utilitzarem la següent taula de valors. La fórmula bàsica per expressar la vulnerabilitat és:

Vulnerabilitat = Freqüència estimada / Dies al any.

Freqüència	ID	Valor	Informació
Extremadament Freqüent	EF	0,9973=364/365	Menys d'una incidència al dia
Molt Freqüent	MF	0,1425=52/365	Menys d'una incidència a la setmana
Freqüent	F	0,0329=12/365	Menys d'una incidència al mes
Normal	FN	0,0055=2/365	Menys d'una incidència cada mig any
Poca	PF	0,0027=1/365	Menys d'una incidència al any
Extremadament Poca	EPF	0,0003=1/(10*365)	Menys d'una incidència cada deu anys

La següent taula també ens servirà per valorar l'impacte que té l'amenaça, en cas de ocasionar-se, sobre l'actiu.

Valor	Impacte	ID	Definició
90%	Crític	C	90% de degradació
75%	Alt	A	75% de degradació
50%	Mig	M	50% de degradació
20%	Baix	B	20% de degradació

En la següent taula podem veure la llista d'amenaces, juntament amb la seva font, origen, motivació i quina acció o repercussió pot tenir sobre els sistemes o l'empresa Cotecom. Al mateix temps, aquestes amenaces estan classificades en quatre categories.

- Accidents (ACC): Situacions que no han sigut provocades i que difícilment poden evitar-se, generalment produïdes per efectes de la natura.
- Errors (ERR): Situacions comeses de forma involuntària durant el desenvolupament de les activitats de l'organització.
- Amenaces intencionades presencials (AIP): Provocades pel personal intern amb la intenció de provocar danys a nivell físic o lògic.
- Amenaces intencionades remotes (AIR): Provocades per terceres persones amb la finalitat de danyar l'organització.

		Font					
ID	AMENAÇA	NATURAL	HUMNA	ENTORN	ORIGEN	MOTIVACIÓ	ACCIÓ
AIP1	Robatori d'informació confidencial		x		Treballadors descontents o deslleial	Obtenció de beneficis econòmics o d'informació	Accés al sistema de manera no autoritzada per a robar informació
AIP2	Danys per aigua	x			Desastre natural, sabotatge, avaria, error d'us...	Per provocar danys o no intencionat.	Inutilització de sistemes i instal·lacions.
AIP3	Manipulació de hardware		x		Treballadors, personal contractat o externs.	Provocar danys	Inutilització de sistemes i instal·lacions.
AIP4	Foc intencionat		x		Sabotatge,..	Per provocar danys	Inutilització de sistemes i instal·lacions.
AIP5	Alteració de dades		x		Treballadors descontents o deslleial	Obtenció de beneficis econòmics o d'informació	Alteració de la informació per provocar danys.

AIP6	Destrucció d'informació		x		Treballadors descontents o deslleial.	Obtenció de beneficis econòmics o d'informació	Destrucció de la informació per provocar danys.
AIP7	Abús de privilegis d'accés		x		Treballadors	Obtenció d'informació confidencial	Accés al sistema de manera no autoritzada per a robar informació
AIP8	Robatori de hardware		x		Treballadors, personal contractat o externs.	Obtenció de beneficis econòmics o d'informació	Subtracció de hardware.
AIP8	Accés no autoritzar		x		Treballadors descontents o deslleial	Obtenció de beneficis econòmics o d'informació	Accés de manera no autoritzada a llocs o informació confidencials
AIR1	Infecció de virus i/o malware		x		No determinat	Obtenció de beneficis econòmics o d'informació	Introduir codi maliciós als sistemes de l'empresa
AIR2	Recepció de correu brossa		x		No determinat	Obtenció de beneficis econòmics o d'informació	Enviament/recepció de correu brossa (SPAM)
AIR3	Atac DoS		x		No determinat	Obtenció de beneficis econòmics o d'informació	Denegació de servei i caiguda de serveis de l'empresa
AIR4	Espionatge industrial		x		Competència	Obtenció d'informació confidencial	Obtenció de dades industrials per personal aliè a l'empresa.
ACC1	Pluges				Desastre natural	Cap, no intencionat	Inutilització de sistemes i instal·lacions.
ACC2	Foc	x			Mal funcionament, error d'us, avaria...	No intencionat.	Inutilització de sistemes i instal·lacions.
ACC3	Terratrèmol	x			Desastre natural	Cap, no intencionat	Inutilització de sistemes i instal·lacions.
ACC4	Averies físiques de hardware			x	No determinat	Cap, no intencionat	pèrdua de disponibilitat
ACC5	Fallada de serveis de comunicació			x	No determinat	Cap, no intencionat	pèrdua de disponibilitat
ACC6	Fallada elèctrica			x	No determinat	Cap, no intencionat	pèrdua de disponibilitat
ERR1	Errors de configuració		x		Treballadors	Cap, no intencionat	Error de configuració dels sistemes per part dels treballadors.
ERR2	Errors humans		x		Treballadors	Cap, no intencionat	Error humà dels treballadors al realitzar una tasca al sistema
ERR3	Errors d'administradors		x		Treballadors	Cap, no intencionat	Error humà dels administradors al realitzar una tasca al sistema
ERR4	Error d'aplicació			x	No determinat	Cap, no intencionat	Errors d'aplicació en el seu funcionament, pèrdua de dades, consistència...
ERR5	Error de sistema			x	No determinat	Cap, no intencionat	Errors de sistema en el seu funcionament, pèrdua de dades, consistència...

Càlcul del risc intrínsec

Es considera que risc intrínsec és la pèrdua anual o diària esperada considerant que no existeixen salvaguardes que protegeixin els actius de les seves amenaces.

La pèrdua anual es calcula tenint en compte:

- El valor dels actius.
- L'exposició dels actius a les amenaces, mesura que sobté de la freqüència d'afectació de l'amenaça sobre l'actiu i el percentatge de degradació que aplica l'amenaça.

Valoració de salvaguardes

Les salvaguardes són les mesures establertes per Cotecom per reduir els seus riscos. Aquestes poden reduir la probabilitat d'èxit d'una amenaça reduint la seva freqüència i/o el seu impacte en cas de produir-se sobre d'un actiu.

L'eficàcia d'una salvaguarda per una determinada amenaça i actiu d'informació es mesura en el percentatge de reducció de la probabilitat i l'impacte. En la següent taula es veu el cost de la salvaguarda, el cost respecte els actius que cobreix i el cost respecte l'amenaça que soluciona.

Nº	Codi	Descripció	Cost	Nº actius	Cost sv / actiu	Nº amenaces	Cost total sv / amenaça
1	SG-001	Sistema alarma incendi i robatori	2.500,0 €	429	5,8 €	3	833,3 €
2	SG-002	Extintors	300,0 €	429	0,7 €	2	150,0 €
3	SG-003	Manteniment línia de dades	2.500,0 €	4	625,0 €	3	833,3 €
4	SG-004	Contractes de confidencialitat per els treballadors	600,0 €	350	1,7 €	5	120,0 €
5	SG-005	Manteniment Google	4.500,0 €	1	4.500,0 €	3	1.500,0 €
6	SG-006	Manteniment de la centre de copiat	500,0 €	7	71,4 €	4	125,0 €
7	SG-007	Sistema de refrigeració	5.000,0 €	14	357,1 €	2	2.500,0 €
8	SG-008	Claus d'accés al CPD i sala de comunicacions.	1,0 €	2	0,5 €	2	0,5 €
9	SG-009	Manteniment general	30.000,0 €	4	7.500,0 €	3	10.000,0 €
10	SG-010	Sistemes SAI	1.500,0 €	16	93,8 €	1	1.500,0 €
11	SG-011	Contracte confidencialitat proveïdors o contractats.	600,0 €	5	120,0 €	4	150,0 €
12	SG-012	Manteniment Generador	1.200,0 €	1	1.200,0 €	4	300,0 €
13	SG-013	Manteniments Firewalls	1.500,0 €	2	750,0 €	4	375,0 €
14	SG-014	Destructora de paper	200,0 €	2	100,0 €	2	100,0 €
15	SG-015	Manteniment Equipament de Xarxa	2.750,0 €	30	91,7 €	4	687,5 €
16	SG-016	Manteniment Cabines de dades	2.500,0 €	4	625,0 €	4	625,0 €
17	SG-017	Manteniment Hadware Servidors	4.500,0 €	7	642,9 €	4	1.125,0 €
18	SG-018	Sistema copies de seguretat	1.350,0 €	3	450,0 €	6	225,0 €
19	SG-019	Antivirus	500,0 €	3	166,7 €	2	250,0 €
20	SG-020	Vídeo Càmeres	500,0 €	1	500,0 €	3	166,7 €
21	SG-021	Manteniment SAP	5.000,0 €	1	5.000,0 €	3	1.666,7 €
22	SG-022	Manteniment PLM	5.000,0 €	1	5.000,0 €	3	1.666,7 €
23	SG-023	Manteniment Alfresco	2.000,0 €	1	2.000,0 €	3	666,7 €
24	SG-024	Manteniment ESXi	1.500,0 €	4	375,0 €	3	500,0 €
25	SG-025	Manteniment Solaris	1.500,0 €	2	750,0 €	3	500,0 €

26	SG-026	Guarda de seguretat	20.000,0 €		429	46,6 €		6	3.333,3 €
27	SG-027	Sistema antiincendi	5.000,0 €		13	384,6 €		2	2.500,0 €

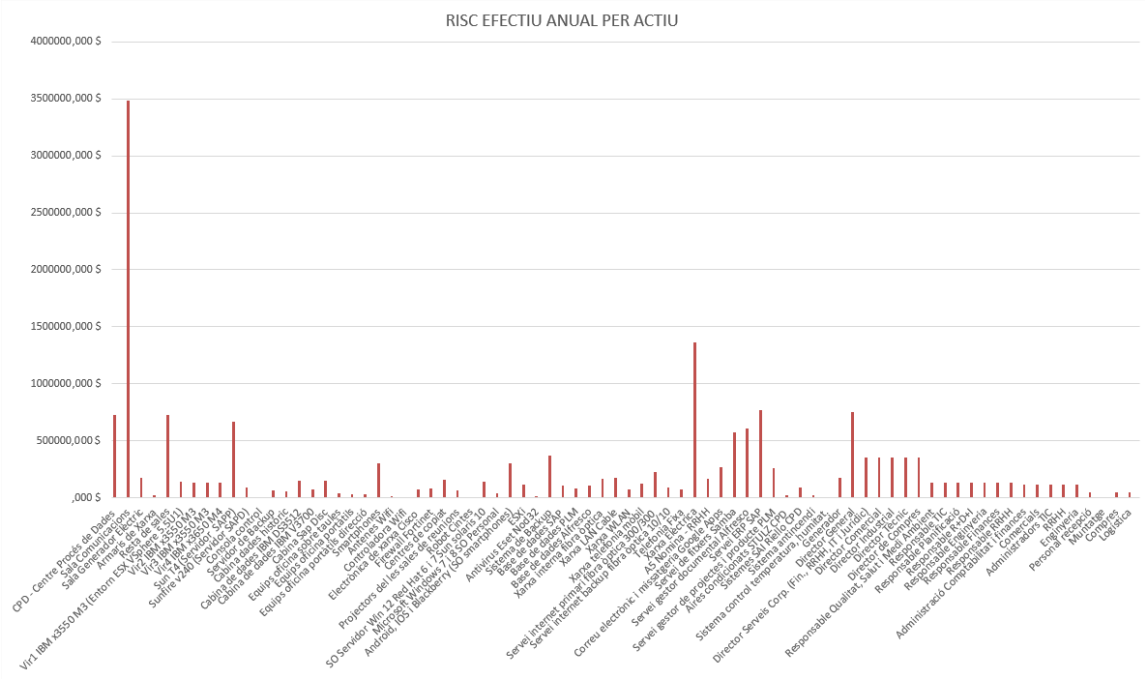
Càlcul risc efectiu

Es considera risc efectiu a la pèrdua anual esperada considerant l'efecte de les salvaguardes actualment implantades per protegir els actius d'informació de les seves amenaces.

La pèrdua anual es calcula tenint en compte:

- El valor dels actius d'informació
- L'exposició dels recursos de la informació a les amenaces, mesurada en termes de freqüència i percentatge de degradació.
- L'eficàcia de les salvaguardes per reduir la freqüència o impacte de les amenaces, tenint en compte com estan implantades.

Podem trobar, doncs, que el risc efectiu anual per actiu és el que es representa en la següent gràfica.



Gestió del Risc

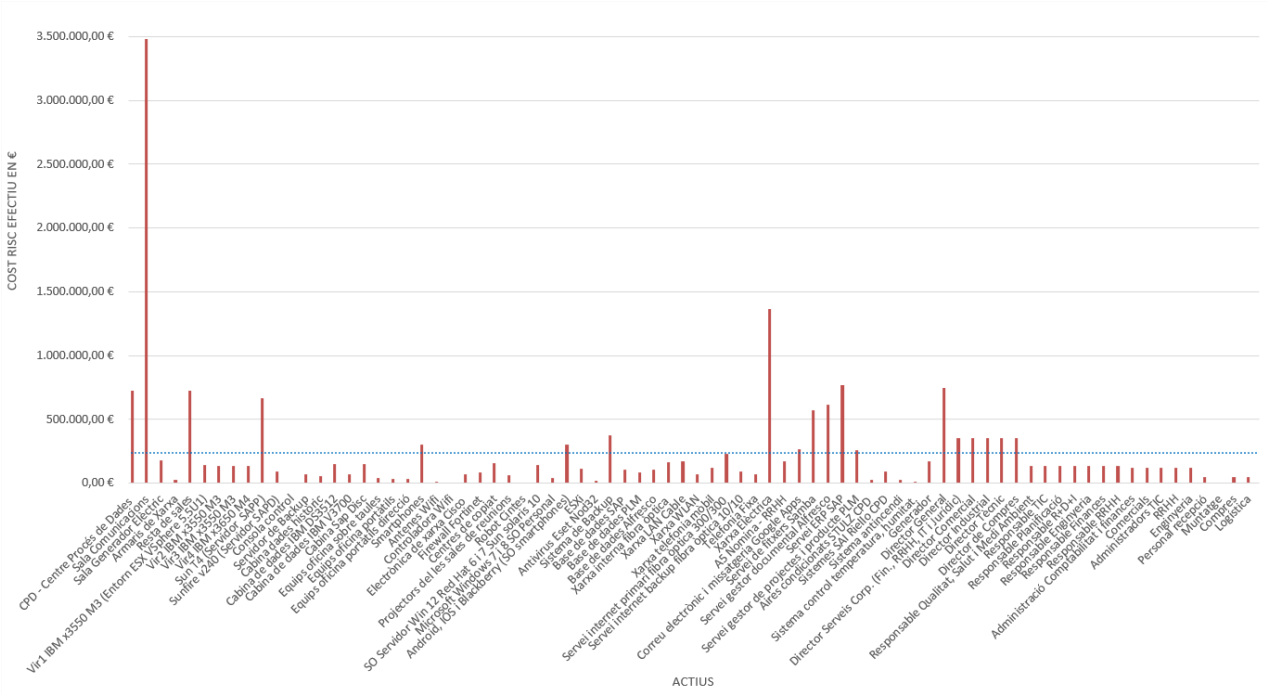
Una vegada identificats i quantificats els riscos de seguretat, cal definir el pla de la seva gestió i reducció.

Al no ser possible la reducció total dels riscos, es necessari definir un nivell de risc que es consideri acceptable per part de Cotecom. Aquesta decisió ha de ser presa per Direcció i serà l'element determinant en l'elaboració dels plans per reduir els riscos.

La decisió presa en aquest projecte és la d'agafar la mitja com a nivell de risc acceptable. Tot el que estigui per sota d'aquest nivell de risc no suposarà una amenaça important per a Cotecom, i per tant no ens interessarà. Al contrari, si el nivell de risc supera al nivell acceptable, en aquest cas haurem d'establir controls per reduir-ho.

Tal com s'ha comentat anteriorment, no és possible la reducció total dels riscos, existeix un risc que continua existint després d'aplicar els controls de seguretat, aquest risc s'anomena Risc Residual.

En la següent gràfica es veu els actius amb els seu valor de risc efectiu, en vermell, i en blau es marca el llindar que marca el risc permès respecte el risc que cal solucionar.



A continuació es pot veure la llistat d'actius que estan per sobre de la mitjana o Risc Residual

Actiu	Risc Efectiu Actiu	Risc Efectiu Mitja
CPD – Centre Procés de dades	727.080,00€	235.887,57 €
Sala Comunicacions	3.482.100,00 €	235.887,57 €
Resta de Sales	726.395,63 €	235.887,57 €
Sun T4 (Servidor SAPP)	666.490,00 €	235.887,57 €
Sistema de Backup	371.424,00 €	235.887,57 €
Xarxa Elèctrica	1.362.180,00 €	235.887,57 €
Correu electrònic i missatgeria Google Apps	266.085,00 €	235.887,57 €
Servei de fitxers Samba	571.590,00 €	235.887,57 €
Servei gestor documental Alfresco	611.010,00 €	235.887,57 €
Servei ERP SAP	768.690,00 €	235.887,57 €
Servei gestor de projectes i producte PLM	256.230,00 €	235.887,57 €
Director General	748.980,00 €	235.887,57 €
Director Serveis Corp. (Fin., RRHH, IT i Jurídic)	354.780,00 €	235.887,57 €
Director Comercial	354.780,00 €	235.887,57 €
Director Industrial	354.780,00 €	235.887,57 €
Director Tècnic	354.780,00 €	235.887,57 €
Director de Compres	354.780,00 €	235.887,57 €

També podem veure la taula del Risc Efectiu pels actius anteriors i com cada amenaça afecta a cada actiu.

Risc Efectiu			CPD - Centre Procés de Dades	Sala Comunicacions	Resta de sales	Sun T4 (Servidor SAPP)	Sistema de Backup	Xarxa Elèctrica	Correu electrònic i missatgeria Google Apps	Servei de fitxers Samba	Servei gestor documental Alfresco	Servei ERP SAP	Servei gestor de projectes i producte PLM	Director General	Director Serveis Corp. (Fin., RRHH, IT i Jurídic)	Director Comercial	Director Industrial	Director Tècnic	Director de Compres
Nº	Código	AMENAZA	400000,0000	200000,0000	75000,0000	200000,0000	30000,0000	400000,0000	200000,0000	200000,0000	200000,0000	200000,0000	200000,0000	400000,0000	200000,0000	200000,0000	200000,0000	200000,0000	200000,0000
1	AIP1	Robatori d'informació confidencial			0,0027 | 0,9000 182,2500				0,0027 | 0,5000 270,0000	0,0003 | 0,9000 54,0000				0,0003 | 0,9000 108,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000
2	AIP2	Danys per aigua	0,0003 | 0,9000 108,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,5000 11,2500	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 8,1000			0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000							
3	AIP3	Manipulacio de hardware	0,0003 | 0,9000 108,0000	0,0027 | 0,9000 486,0000			0,0003 | 0,2000 1,8000	0,0003 | 0,9000 108,0000											
4	AIP4	Foc intencionat	0,0003 | 0,2000 24,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,5000 11,2500	0,0003 | 0,2000 12,0000													
5	AIP5	Alteració de dades			0,0027 | 0,5000 101,2500					0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 108,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000
6	AIP6	Destrucció d'informació			0,0027 | 0,5000 101,2500					0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000			0,0003 | 0,9000 108,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000
7	AIP7	Abus de privilegis d'acces	0,0003 | 0,9000 108,0000	0,0003 | 0,9000 54,0000	0,0027 | 0,5000 101,2500					0,0027 | 0,9000 486,0000		0,0027 | 0,9000 486,0000		0,0027 | 0,2000 216,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000
8	AIP8	Robatori de hardware			0,0055 | 0,7500 309,3750														
9	AIP9	Acces no autoritzat	0,0003 | 0,9000 108,0000	0,0329 | 0,9000 5922,0000	0,0055 | 0,7500 309,3750							0,0027 | 0,9000 486,0000		0,0027 | 0,2000 216,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000
10	AIP1	Infecció de virus i/o malware												0,0027 | 0,2000 216,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000	0,0027 | 0,2000 108,0000
11	AIP2	Recepció de correu brosa																	
12	AIP3	Atac DoS							0,0003 | 0,9000 54,0000		0,0003 | 0,9000 54,0000								
13	AIP4	Espionatge industrial			0,0055 | 0,7500 309,3750									0,0027 | 0,5000 540,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000
14	ACC1	Pluges	0,0003 | 0,9000 108,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,2000 4,5000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 8,1000	0,0003 | 0,9000 108,0000			0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000						
15	ACC2	Foc	0,0003 | 0,2000 24,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,5000 11,2500	0,0003 | 0,2000 12,0000		0,0003 | 0,9000 108,0000											
16	ACC3	Terratremol	0,0003 | 0,9000 108,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 20,2500	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 8,1000	0,0003 | 0,9000 108,0000			0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000	0,0003 | 0,9000 54,0000						
17	ACC4	Averies fisiques de hardware				0,0003 | 0,9000 54,0000													
18	ACC5	Fallada de serveis de comunicació	0,0027 | 0,5000 540,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 101,2500				0,0027 | 0,7500 405,0000										
19	ACC6	Fallada electrica	0,0027 | 0,5000 540,0000	0,0027 | 0,5000 270,0000	0,0055 | 0,9000 371,2500														
20	ERR1	Errors de configuració			0,0003 | 0,5000 11,2500														
21	ERR2	Errors humans	0,0003 | 0,9000 108,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,5000 11,2500			0,0055 | 0,7500 1650,0000		0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000	0,0027 | 0,9000 486,0000	0,0027 | 0,5000 540,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000	0,0027 | 0,5000 270,0000
22	ERR3	Errors d'administradors	0,0003 | 0,9000 108,0000	0,0027 | 0,9000 486,0000	0,0003 | 0,5000 11,2500	0,0027 | 0,9000 486,0000	0,0003 | 0,5000 4,5000												
23	ERR4	Error d'aplicació				0,0055 | 0,5000 550,0000	0,0329 | 0,5000 493,5000												
24	ERR5	Error de sistema			0,0003 | 0,5000 11,2500	0,0055 | 0,5000 550,0000	0,0329 | 0,5000 493,5000	0,0055 | 0,7500 1650,0000			0,0027 | 0,9000 486,0000								
		Risc efectiu diari per actiu	**1.992,00 €**	**9.540,00 €**	**1.990,13 €**	**1.826,00 €**	**1.017,60 €**	**3.732,00 €**	**729,00 €**	**1.566,00 €**	**1.674,00 €**	**2.106,00 €**	**702,00 €**	**2.052,00 €**	**972,00 €**	**972,00 €**	**972,00 €**	**972,00 €**	**972,00 €**
		Risc efectiu anual per actiu	**727.080,00 €**	**3.482.100,00 €**	**726.395,63 €**	**666.490,00 €**	**371.424,00 €**	**1.362.180,00 €**	**266.085,00 €**	**571.590,00 €**	**611.010,00 €**	**768.690,00 €**	**256.230,00 €**	**748.980,00 €**	**354.780,00 €**	**354.780,00 €**	**354.780,00 €**	**354.780,00 €**	**354.780,00 €**
		Mitja Anual del risc efectiu	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**	**235.887,57 €**

Conclusions

Sobre els actius de l'empresa Cotecom s'ha realitzat un anàlisis de risc. Aquest anàlisis ha consistit en aplicar sobre el valor de cada actiu una penalització segons la freqüència i la degradació que aplica cada amenaça que l'afecta. En el nostre cas, tot i valorar les salvaguardes actuals, quan s'ha realitzat el cost del risc de sobre cada actiu, aquest ja inclou les salvaguardes existents, de manera que obtenim directament el cost del risc efectiu per a cada actiu.

Un cop obtingut aquest risc s'ha decidit utilitzar la mitjana del risc efectiu anual com a valor de tria dels actius que estan per sobre del risc residual, sobre els quals cal aplicar controls específics per a disminuir aquest risc efectiu i estudiar aquests actius per saber quines propostes de projectes es faran per a reduir-lo.

Proposta de Projectes

Introducció

En el capítol anterior s'ha realitzat l'anàlisi de risc per saber el nivell de risc actual de Cotecom, amb el resultat d'aquest anàlisi ha arribat el moment de plantejar els projectes per a millorar l'estat de la seguretat de l'organització.

La proposta de projectes serà el resultat d'agrupar un conjunt de recomanacions identificades, a la fase d'anàlisis de riscos, per facilitar la seva execució. No només s'entrarà en la millora en la gestió de seguretat i compliment de la normativa ISO, sinó també, en possibles beneficis col·laterals com poden ser optimització de recursos, millora de gestió de processos i tecnologies presents a l'organització.

Estructura proposta de projectes

Els projectes han de quantificar-se econòmicament i planificar-se en el temps, establint períodes de consecució dels objectius (en general, curt, mig i llarg termini). També s'han d'incloure punts de control en la planificació que permetran considerar realment el Pla d'Implantació del SGSI com un procés de millora continua.

El contingut de cada pla de projectes és:

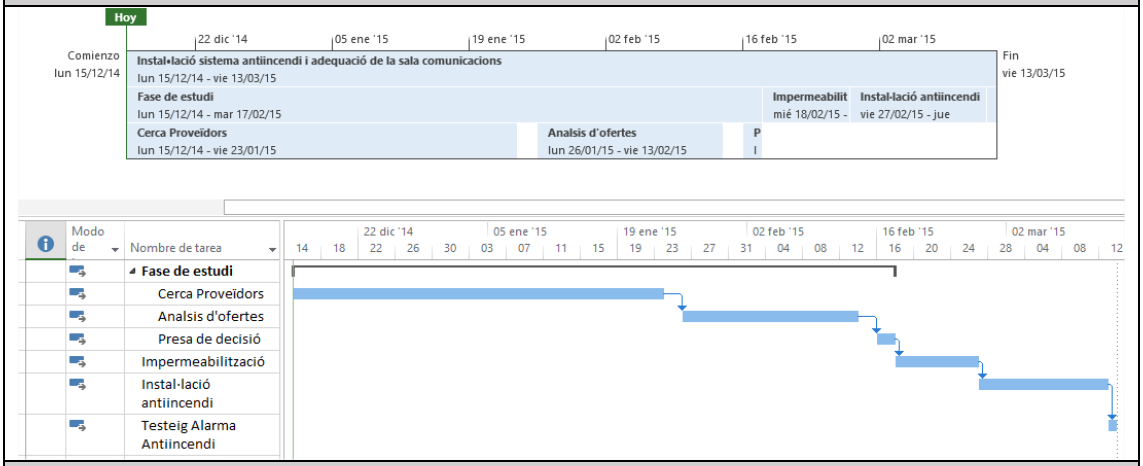
- Projecte: Títol o nom de projecte.
- Introducció: Inclourà una referencia al projecte d'anàlisi de risc i els seus resultats, que explicarà el perquè de la seva proposta.
- Objectiu: Conjunt de salvaguardes a implantar.
- Abast: Definició de l'entorn on s'implantaran les diferents salvaguardes i el nivell de millora que es vol obtenir a cada una d'elles.
- Enfoc: Principals tasques i activitats que formaran part del projecte.
- Planificació: Temps necessari per l'execució del projecte i principals fites intermitges.
- Pressupost: Estimació dels costos necessaris per a l'execució del projecte.

Proposta de Projectes

Els projectes proposats apareixen arrel del quadre de Risc Efectiu que s'ha obtingut de l'anàlisi de risc, aquests projectes proposaran millores als actius que estan per sobre del llindar permès.

Projecte: P1 - Documentació CPD
Introducció:
Les principals amenaces del CPD, són error d'administradors, errors humans i manipulació de hardware, aquests problemes venen deguts en gran mesura a la manca de documentació de com esta connectat el CPD.
Abast:
El CPD, i tot el que contingui (servidors, SAI's, cabines de disc, electrònica de xarxa, connexions elèctriques...)

Objectiu:
Documentar correctament les connexions de xarxa, entre servidors, cabines de disc, connexions elèctriques i SAI's dels actius que hi ha al CPD per tal de reduir el risc d'errors humans, error d'administradors i manipulació de hardware.
Enfoc:
Analitzar com estan muntats a nivell de hardware i cablejat (de xarxa, elèctric, cablejat específic dels actius del CPD) Dibuixar esquemes de dependències. Documentar manteniments i garanties associades als serveis que ofereixen els diferents actius. Definir una política d'accés.
Planificació:
No hi ha planificació, executar tant aviat com sigui possible.
Pressupostos:
No hi ha pressupost ja que es feina interna, executada pel personal del departament.
ISO 27002
Obtenim millores en: A.11.1.1 Perímetres de seguretat física A.11.1.2 Controls físics d'entrada A.11.1.4 Protecció contra les amenaces externes i ambientals A.11.1.3 Seguretat d'oficines, despatxos i recursos. A.11.2.1 Localització i protecció d'equips A.11.2.3 Seguretat del cablejat A.11.2.4 Manteniment dels equips A.12.1.1 Documentació de procediments d'operació

Projecte: P2 - Instal·lació sistema antiincendi i adequació de la sala comunicacions.
Introducció:
La sala de comunicacions es veu afectada per amenaces com foc o risc d'incendi i danys per aigua i pluja, davant aquests perills cal adequar millor aquesta sala.
Abast:
Abast del projecte és la sala de comunicacions i el seu contingut, electrònica de xarxa, Firewalls Fortinet, línies de dades i línia de telefònica.
Objectiu:
Per adequar la sala de comunicacions per tal de reduir el risc de foc o incendi, danys per aigua i pluja.
Enfoc: - Instal·lació d'un sistema antiincendi. - Impermeabilització del sostre i parets de la sala per evitar possibles problemes per pluja o per les canonades que passen adjacents a la sala.
Planificació:

Pressupostos:

- 2,500€ Sistema antiincendi.
- 1,500€ impermeabilització sostre i parets de la sala.

ISO 27002

A.11.1.4 Protecció contra les amenaces externes i ambientals

Projecte: P3 - Formació dels empleats.

Introducció:

Un dels principals problemes que han aparegut en la matriu de risc fa referencia a la protecció de les dades, per exemple, el robatori d'informació confidencial, alteració de dades, destrucció d'informació, accés no autoritzat, espionatge industrial.

Per això es creu que seria bo formar a els empleats de Cotecom en matèries bàsiques de seguretat de la informació i LOPD.

Abast:

Tots els empleats de Cotecom.

Objectiu:

Formació bàsica i conscienciació a nivell d'usuari sobre seguretat de la informació i la llei orgànica de protecció de dades.

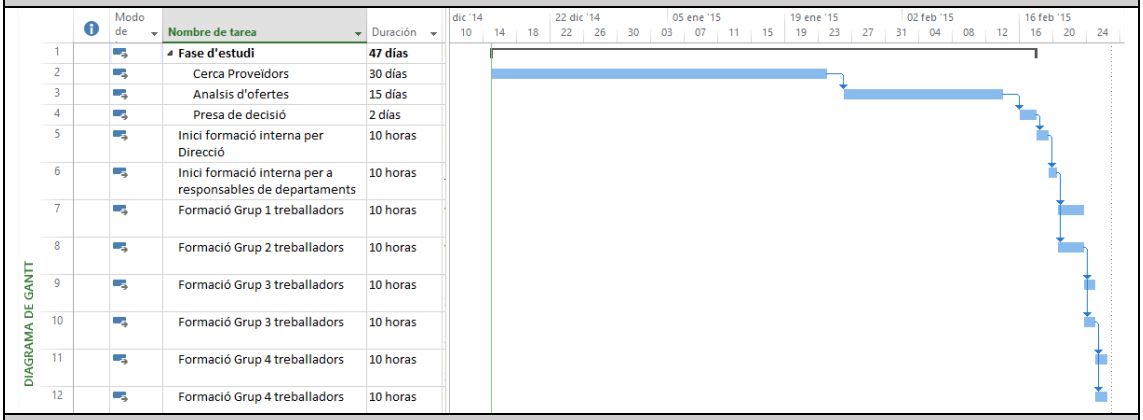
- Millora de la conscienciació de les millors pràctiques al lloc de treball
- Millora en el coneixement de la documentació referent a LOPD de l'empresa
- Millora en la formació de noves tècniques de seguretat
- Reducció de les incidències amb el personal de l'empresa

Enfoc:

Establir una seria de formacions internes per nivells de usuaris i funcions.

- Direcció
- Responsables
- Treballadors segons funcions

Planificació:



Pressupostos:

El cost d'aquesta formació per a la gent d'oficina, 120 persones, és de 3500€

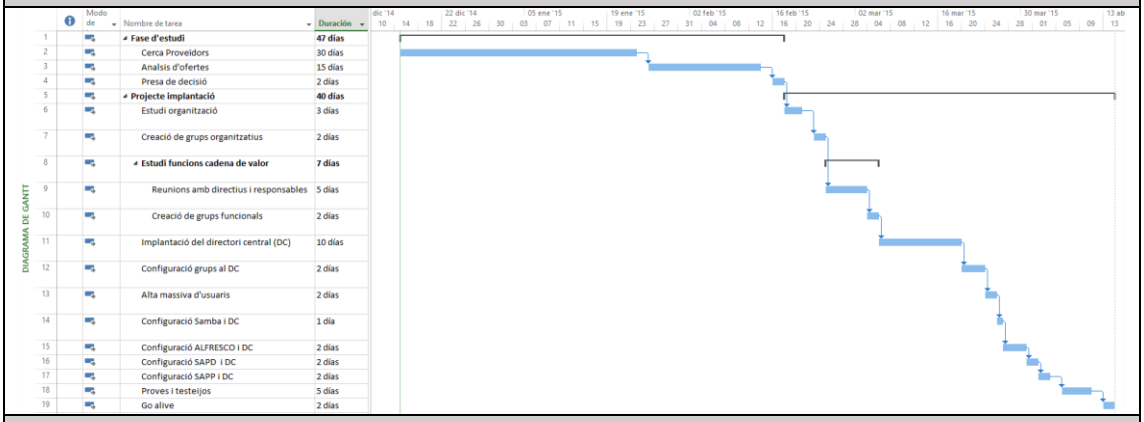
ISO 27002

A.5.1.1 Conjunt de polítiques per la seguretat de la informació
A.5.1.2 Revisió de les polítiques per la seguretat de la informació
A.11.1.3 Seguretat d'oficines, despatxos i recursos.
A.11.2.9 Política de treball net i bloqueig de pantalla.

Projecte: P4 - Directori central d'usuaris

Introducció:

A dia d'avui, Cotecom no té cap directori centralitzat d'usuaris, això fa que cada sistema tingui els

seus propis grups i rols, produint moltes vegades errors d'assignació de permisos, ja que es fa molt complicat administrar-los davant de canvis de lloc de treball, incorporacions o baixes.
Abast:
Els sistemes de Cotecom Google apps, SAP, Alfresco, samba, SO Windows 7 i 8.1 i PLM, i els seus usuaris.
Objectiu:
Implantar un sistema centralitzat d'usuaris, que vagi lligat als serveis de Cotecom, i que reguli els grups, rols i permisos d'accés dels usuaris de Cotecom, i la seva autenticació a aquests (single sign on)
Enfoc:
Estudiar les diferents solucions de mercat en matèries de directori central d'usuaris (LDAP, Active Directory, Oracle...) i implantar a nivell corporatiu una solució de single sign on.
Planificació:

Pressupostos:
El pressupost estimat per aquest projecte és de 50.000€.
ISO 27002
A.9.1.1 Política de control d'accessos A.9.2.2 Gestió dels drets d'accés assignats a usuaris A.9.2.5 Revisió dels drets d'accés dels usuaris A.9.4.1 Restricció d'accés a la informació A.9.4.2 Procediments segurs d'inici de sessió A.9.4.3 Gestió de contrasenyes d'usuari A.10.1.1 Política d'us dels controls criptogràfics A.10.1.2 Gestió de Contrasenyes.

Projecte: P5 - Millores Xarxa Elèctrica
Introducció:
Millorar la xarxa elèctrica de Cotecom per reduir el nivell d'incidències.
Abast:
Instal·lació elèctrica de Cotecom
Objectiu:
Millorar la infraestructura elèctrica de Cotecom, i així evitar errades en la manipulació de hardware, errors humans i errors de sistema.
Enfoc:
Analitzar la infraestructura elèctrica i procediments relacionats amb ella. Millorar la documentació associada a la infraestructura elèctrica. Aplicar tests anuals i trimestrals de revisió i verificació de l'equipament elèctric i les seves salvaguardes.
Planificació:
La planificació d'aquest projecte està sotmesa a les irregularitats que es trobin en la xarxa elèctrica interna, de manera que es seguirà el següent pla de treball que s'executarà pel propi departament de

manteniment de l'empresa. Juntament al departament de manteniment, s'ha acordat el següent pla de treball:

- Revisió de la infraestructura elèctrica actual
- Informe d'irregularitats
- Pressupost de reparació de les irregularitats

Un cop realitzat aquest primer estudi es valorarà quines millores seran aplicades i quines no, depenent del cost d'aquestes i la millora que aportin.

Pressupostos:

El pressupost estimat per aquest projecte es de 15.000€.

ISO 27002

A.12.6.1 Gestió de les vulnerabilitats tècniques

Projecte: P6 - Configuració sistema alta disponibilitat per Sun T4 SAPP

Introducció:

L'ERP SAP s'ha convertit en el core de Cotecom, això fa que qualsevol caiguda d'aquest servei sigui de gran afectació per a l'empresa.

Abast:

Tota l'empesa.

Objectiu:

Muntar un sistema d'alta disponibilitat pel servidor Sun T4 de SAP productiu per reduir al màxim possible les fallades de disponibilitat d'aquest servei.

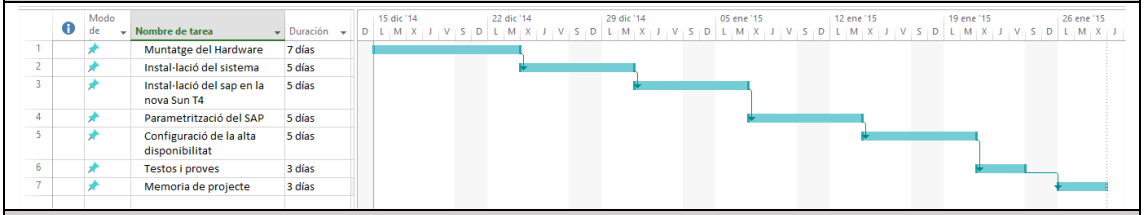
Enfoc:

Amb el proveïdor actual, treballar en la implantació d'un sistema Sap d'alta disponibilitat que permeti reduir al mínim l'impacte de caigudes del sistema.

Hi ha varies maneres de muntar aquesta alta disponibilitat amb un clúster local de dos màquines Sun T4 que mantinguin el servei actiu en cas de caiguda de qualsevol de les dos o una rèplica al núvol que en cas de fallida la màquina principal es pugui utilitzar com a servidor primari.

En aquest cas, després de valorar les dos opcions, s'ha decidit, per un tema de pressupost, muntar un clúster local de dos màquines Sun T4.

Planificació:



	Modo de	Nombre de tarea	Duración
1		Muntatge del Hardware	7 días
2		Instal·lació del sistema	5 días
3		Instal·lació del sap en la nova Sun T4	5 días
4		Parametrització del SAP	5 días
5		Configuració de la alta disponibilitat	5 días
6		Testos i proves	3 días
7		Memoria de projecte	3 días

Pressupostos:

El pressupost 60.000€

ISO 27002

A.17.1.1 Planificació de la continuïtat de la seguretat de la informació
A.17.1.2 Implantació de la continuïtat de la seguretat de la informació
A.17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació
A.17.2.1 Disponibilitat d'instal·lacions per el processament de la informació

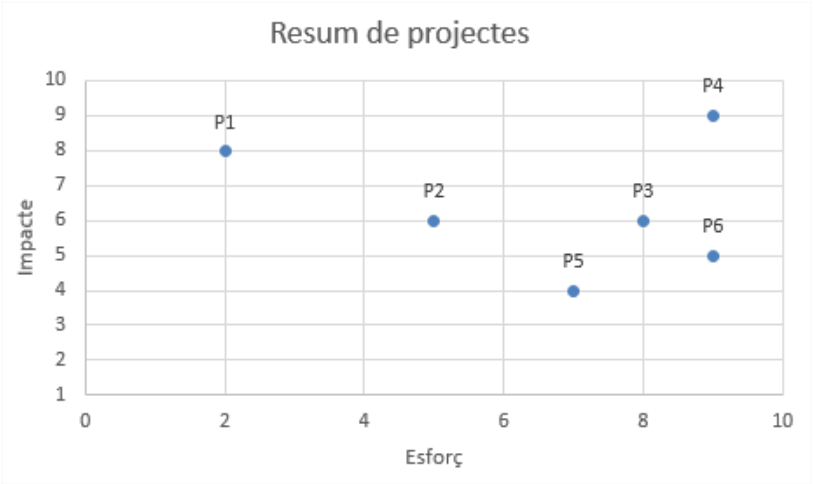
Resum de projectes

Un cop definits els diferents projectes, s'ha realitzat una priorització entre ells, per triar l'ordre d'implantació. Els principals aspectes a considerar per la priorització són:

- Reducció del risc: Els projectes que redueixin el risc en major mesura han d'executar-se tant aviat com sigui possible
- Relació amb altres projectes: Aprofitament de recursos entre projectes o concatenació de projectes aprofitant els resultats dels anteriors o fases intermitges.
- Pressupost i requeriments de recursos pel projecte. Cal valorar el cost i els recursos necessaris per a la implantació del projecte. i disposar del tot el necessari per assegurar l'èxit.

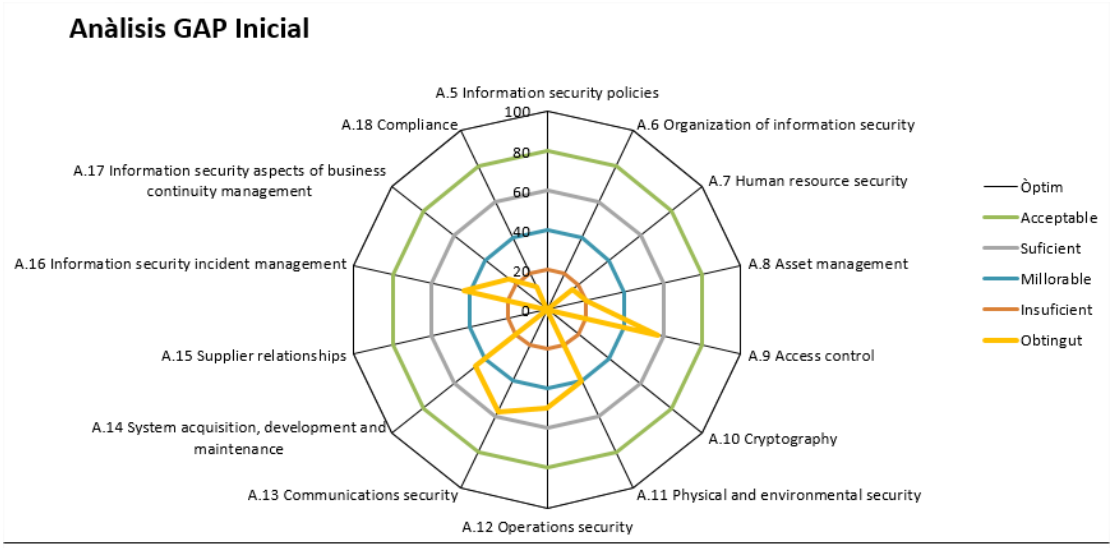
Tenint en compte els anteriors punts, s'han valorat els projectes segons l'esforç d'implantació (Pressupost i requeriments), i l'impacte que tindran sobre l'organització. L'objectiu del proper gràfic és permetre identificar quins són el projectes prioritaris, de manera que, s'implantaran primer els projectes que requereixin menys esforç i tinguin més impacte positiu a Cotecom, sempre i quan no hi hagi dependències entre projectes, per tant apareixeria aquesta tercera variable de relació amb altres projectes.

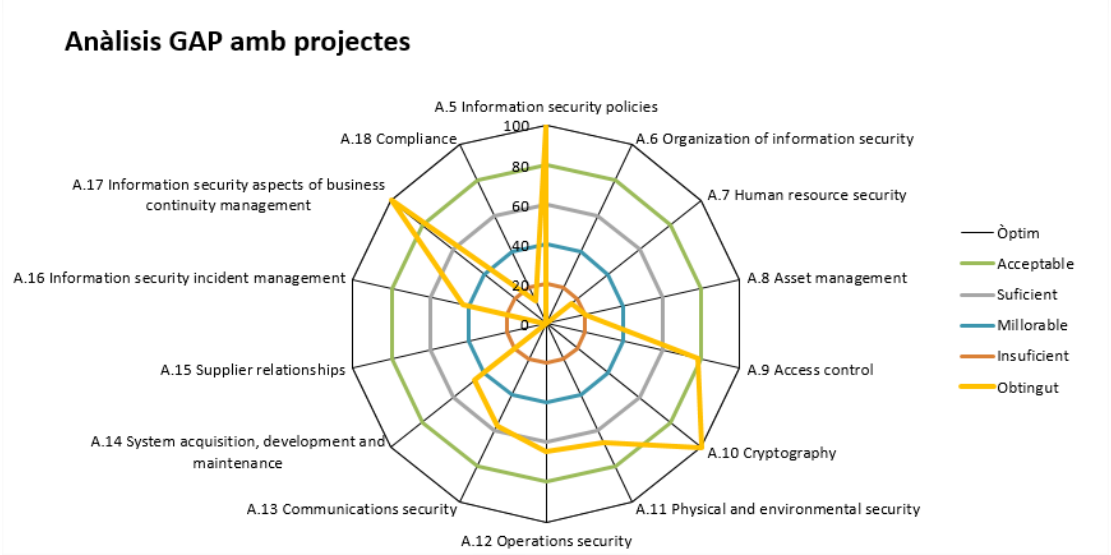
Codi	Impacte	Esforç
P1	8	2
P2	6	5
P3	6	8
P4	9	9
P5	4	7
P6	5	9



Resultats

Una vegada realitzada la proposta dels diferents projectes que volem implantar a l'empresa, cal veure quina millora representen respecte la ISO 27002. Aquesta millora es representa amb un diagrama de radar amb el sumatori de tots els projectes i així poder veure quins són els àmbits de millora globals.





En la primera gràfica podem veure el GAP inicial de compliment dels controls de la ISO 27002 i en la segona gràfica com quedaria la situació després d'aplicar els projectes.

Auditoria de compliment

Introducció

En aquesta part final del projecte coneixem els actius de l'empresa i hem avaluat les amenaces sobre ells, en l'anàlisi de risc. D'aquest anàlisi han aparegut projectes per a resoldre les mancances, on s'ha vist una mostra dels més importants i com s'apliquen sobre la ISO 27002. Ara és el moment de fer una parada i avaluar fins a quin punt l'empresa compleix amb les "bones pràctiques" en matèria de seguretat. Una auditoria amb la ISO 27002 ens servirà com a marc de control de l'estat de la seguretat.

Metodologia

En aquest apartat descriurem breument la metodologia de l'auditoria utilitzada per portar a terme l'anàlisi de maduresa i compliment de la ISO/IEC 27002:2013 sobre els seus 133 controls o mesures preventives sobre les bones pràctiques per a la Gestió de la Seguretat de

la Informació, organitzats en 14 àrees i 35 objectius de control. Aquest estàndard és internacionalment conegut i és perfectament vàlid per a la majoria de les organitzacions.

Hi ha diferents aspectes sobre els quals les mesures preventives actuen reduint el risc:

- Formalització de les pràctiques mitjançant documents escrits o aprovats
- Polítiques del personal de l'empresa.
- Sol·licituds tècniques de programari, maquinari i comunicacions.
- Seguretat física.

Per tal d'avaluar la maduresa de la seguretat de l'organització, s'analitzaran els següents dominis de la ISO/IEC 27002:2013:

- Política de seguretat
- Organització de la seguretat de la informació
- Gestió d'actius
- Seguretat als recursos humans
- Seguretat física i ambiental
- Control d'accés
- Adquisició, desenvolupament i manteniment de Sistemes d'Informació
- Gestió d'incidents
- Gestió de continuïtat de negoci
- Compliment

En l'estudi es realitzarà una revisió dels 133 controls plantejats per la norma a complir, amb els diferents objectius de control. La següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM), ens permet veure la metodologia que s'utilitzarà per descriure el compliment dels diferents controls de la ISO/IEC 27001.

Efectivitat	CMM	Significat	Descripció
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem.
10%	L1	Inicial /Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. Els procediments són inexistents o localitzats en àrees concretes. No existeixen plantilles.
50%	L2	Reproduïble però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca. Es normalitzen les "bones pràctiques" en base a l'experiència i al mètode. No hi ha comunicació o entreteniment formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	L3	Procés definit	L'organització sencera participa al procés. Els processos estan implantats, documentats i comunicats mitjançant entreteniment
95%	L4	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, s'han de tenir eines per a millorar la qualitat i l'eficiència.
100%	L5	Optimitzat	Els processos estan sota constant millora. En base criteris quantitatius es determinem les desviacions més comunes i s'optimitzen els processos.

Taula compliment dels controls ISO/IEC 27002:2013

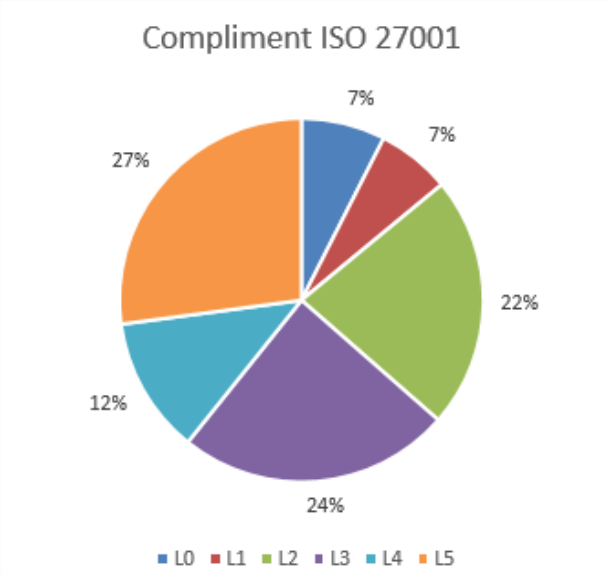
A continuació es veu la taula de compliment de la ISO/IEC 27002:2013, amb els valors de efectivitat i el valor CMM estimat per cada un dels controls.

CONTROL			Efectivitat	CMM
A.5 Política de Seguretat de la Informació			50%	L2
	A.5.1 Directrius de la Direcció en seguretat de la informació		50%	L2
		A.5.1.1 Conjunt de polítiques per la seguretat de la informació	50%	L2
		A.5.1.2 Revisió de les polítiques per la seguretat de la informació	50%	L2
A.6 Organització de la Seguretat de la Informació			26%	L1>L2
	A.6.1 Organització interna			
		A.6.1.1 Assignació de responsabilitats per la seguretat de la informació	10%	L1
		A.6.1.2 Segregació de tasques	50%	L2
		A.6.1.3 Contacte amb les autoritats	10%	L1
		A.6.1.4 Contacte amb grups d'interès especial	0%	L0
		A.6.1.5 Seguretat de la informació en la gestió de projectes	10%	L0
	A.6.2 Dispositius mòbils i teletreball			
		A.6.2.1 Política d'us de dispositius mòbils	50%	L2
		A.6.2.2 Teletreball	50%	L2
A.7 Seguretat dels Recursos humans			56%	L2
	A.7.1 Abans de la contractació		48%	L2
		A.7.1.1 Investigació d'antecedents	50%	L2
		A.7.1.2 Termes i condicions de contractació	90%	L3
	A.7.2 Durant la contractació			
		A.7.2.1 Gestió de les responsabilitats	10%	L1
		A.7.2.2 Conscienciació, educació i capacitació en Seg. de la informació	50%	L3
		A.7.2.3 Procés disciplinari	0%	L0
	A.7.3 Cessament o canvi de lloc de treball			
		A.7.3.1 Cessament o canvi de lloc de treball	90%	L4
A.8 Gestió d'actius			53%	L2
	A.8.1 Responsabilitat sobre els actius			
		A.8.1.1 Inventari d'actius	95%	L5
		A.8.1.2 Propietat dels actius	90%	L3
		A.8.1.3 Us acceptable dels actius	90%	L3
		A.8.1.4 Devolució dels actius	90%	L3
	A.8.2 Classificació de la informació			
		A.8.2.1 Directrius de classificació	50%	L2
		A.8.2.2 Etiquetat i manipulat de la informació	10%	L1
		A.8.2.3 Manipulació dels actius	0%	L0
	A.8.3 Utilització de suports d'emmagatzematge			
		A.8.3.1 Gestió de suports extraïbles	0%	L0
		A.8.3.2 Eliminació de suports	100%	L5
		A.8.3.3 Suports físics en transit	0%	L0
A.9 Control d'accés			73%	L2>L3
	A.9.1 Requisits del negoci per el control d'accés			
		A.9.1.1 Política de control d'accessos	90%	L3
		A.9.1.2 Control d'accés a les xarxes i serveis associats	95%	L4
	A.9.2 Gestió d'accés d'usuari			
		A.9.2.1 Gestió d'altes/baixes en el registre d'usuaris	90%	L3
		A.9.2.2 Gestió dels drets d'accés assignats a usuaris	90%	L3
		A.9.2.3 Gestió dels drets d'accés amb privilegis especials	90%	L3
		A.9.2.4 Gestió de informació confidencial d'autenticació d'usuaris.	90%	L3
		A.9.2.5 Revisió dels drets d'accés dels usuaris.	90%	L3
		A.9.2.6 Retirada o adaptació dels drets d'accés	95%	L4
	A.9.3 Responsabilitat dels Usuaris			
		A.9.3.1 Ús de la informació confidencial per l'autenticació	10%	L1

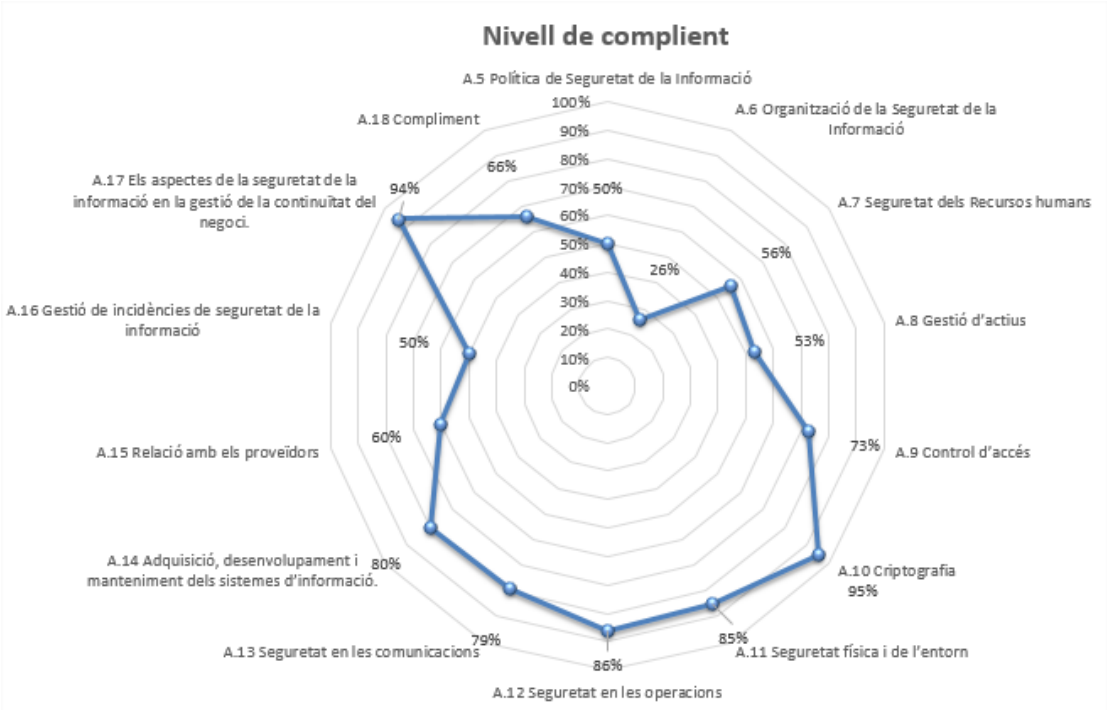
A.9.4 Control d'accés a sistemes i aplicacions				
	A.9.4.1	Restricció d'accés a la informació	95%	L4
	A.9.4.2	Procediments segurs d'inici de sessió	50%	L2
	A.9.4.3	Gestió de contrasenyes d'usuari	90%	L3
	A.9.4.4	Us d'eines d'administració de sistemes	50%	L2
	A.9.4.5	Control d'accés al codi font dels programes		
A.10 Criptografia			95%	L4
A.10.1 Xifrat				
	A.10.1.1	Política d'us dels controls criptogràfics	95%	L4
	A.10.1.2	Gestió de contrasenyes	95%	L4
A.11 Seguretat física i de l'entorn			85%	L3
A.11.1 Àrees segures.				
	A.11.1.1	Perímetres de seguretat física.	100%	L5
	A.11.1.2	Controls físics d'entrada.	100%	L5
	A.11.1.3	Seguretat d'oficines, despatxos i recursos.	90%	L3
	A.11.1.4	Protecció contra les amenaces externes i ambientals.	100%	L5
	A.11.1.5	El treball en àrees segures.	95%	L4
	A.11.1.6	Àrees d'accés públic, carga i descarrega.	90%	L3
A.11.2 Seguretat dels equips				
	A.11.2.1	Localització i protecció d'equips.	100%	L5
	A.11.2.2	Instal·lacions de subministres.	100%	L5
	A.11.2.3	Seguretat del cablejat.	100%	L5
	A.11.2.4	Manteniment dels equips.	100%	L5
	A.11.2.5	Sortida d'actius fora de les dependències de l'empresa	10%	L1
	A.11.2.6	Seguretat dels equips i actius fora de les instal·lacions.	50%	L2
	A.11.2.7	Reutilització o retirada segura dels dispositius d'emmagatzematge	100%	L5
	A.11.2.8	Equip informàtic d'usuari desatès.	50%	L2
	A.11.2.9	Política de lloc de treball net i bloqueig de pantalla	90%	L3
A.12 Seguretat en les operacions			86%	L3
A.12.1 Responsabilitat i procediments d'operació				
	A.12.1.1	Documentació de procediments d'operació.	100%	L5
	A.12.1.2	Gestió de canvis.	95%	L4
	A.12.1.3	Gestió de capacitats.	90%	L3
	A.12.1.4	Separació d'entorns de desenvolupament, prova i producció.	100%	L5
A.12.2 Protecció contra codi maliciós.				
	A.12.2.1	Controls contra codi maliciós.	95%	L4
A.12.3 Copies de seguretat.				
	A.12.3.1	Copies de seguretat de la informació.	100%	L5
A.12.4 Registre de l'activitat i supervisió.				
	A.12.4.1	Registre i gestió d'esdeveniments d'activitat.	90%	L3
	A.12.4.2	Protecció dels registres d'informació.	100%	L5
	A.12.4.3	Registres d'activitat de l'administrador i operador de sistemes.	50%	L2
	A.12.4.4	Sincronització de rellotges.	100%	L5
A.12.5 Control del software en explotació				
	A.12.5.1	Instal·lació del software en sistemes en explotació	50%	L2
A.12.6 Gestió de la vulnerabilitat tècnica.				
	A.12.6.1	Gestió de les vulnerabilitats tècniques.	95%	L4
	A.12.6.2	Restriccions en la instal·lació de software.	50%	L2
A.12.7 Consideracions de les auditories dels sistemes d'informació.				
	A.12.7.1	Controls d'auditoria dels sistemes d'informació.	90%	L3
A.13 Seguretat en les comunicacions			79%	L2>L3
A.13.1 Gestió de la seguretat en les xarxes				
	A.13.1.1	Controls de xarxa	100%	L5
	A.13.1.2	Mecanismes de seguretat associats a els serveis de xarxa.	100%	L5
	A.13.1.3	Segregació de Xarxes	100%	L5
A.13.2 Intercanvi d'informació amb parts externes.				
	A.13.2.1	Polítiques i procediments d'intercanvi d'informació.	50%	L2
	A.13.2.2	Acords d'intercanvi.	50%	L2

	A.13.2.3	Missatgeria electrònica.	50%	L2
	A.13.2.4	Acords de confidencialitat i secret	100%	L5
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.			80%	L3
A.14.1 Requisits de seguretat dels sistemes d'informació.				
	A.14.1.1	Anàlisis i especificacions dels requisits de seguretat.	90%	L3
	A.14.1.2	Seguretat en les comunicacions en serveis accessibles per xarxes publiques.	100%	L5
	A.14.1.3	Protecció de les transaccions per xarxes de comunicacions.	100%	L5
A.14.2 Seguretat ens els processos de desenvolupament i suport				
	A.14.2.1	Polítiques de desenvolupament segur de software.	NO APLICA	
	A.14.2.2	Procediments de control de canvis en els sistemes.	90%	L3
	A.14.2.3	Revisió tècnica de les aplicacions després de fer canvis en el SO.	90%	L3
	A.14.2.4	Restriccions en els canvis en els paquets de software.	90%	L3
	A.14.2.5	Us de principis d'enginyeria en protecció de sistemes.	NO APLICA	
	A.14.2.6	Seguretat en entorns de desenvolupament	90%	L3
	A.14.2.7	Externalització del desenvolupament de software	95%	L4
	A.14.2.8	Proves de funcionalitat durant el desenvolupament de sistemes	100%	L5
	A.14.2.9	Proves d'acceptació.	100%	L5
A.14.3 Prova de dades				
	A.14.3.1	Protecció de les dades utilitzades en proves.	100%	L5
A.15 Relació amb els proveïdors			60%	L3
A.15.1 Seguretat de la informació en les relacions amb proveïdors.				
	A.15.1.1	Política de seguretat de la informació per proveïdors.	50%	L2
	A.15.1.2	Tractament del risc dintre d'acords de proveïdors.	50%	L2
	A.15.1.3	Cadena de subministrament en tecnologies de la informació i comunicacions.	NO APLICA	
A.15.2 Gestió de la prestació del servei per proveïdors.				
	A.15.2.1	Supervisió i revisió dels serveis prestats per tercers.	100%	L5
	A.15.2.2	Gestió de canvis en els serveis prestats per tercers.	100%	L5
A.16 Gestió de incidències de seguretat de la informació			50%	L2
A.16.1 Gestió de incidències de seguretat de la informació				
	A.16.1.1	Responsabilitats i procediments.	10%	L1
	A.16.1.2	Notificació dels esdeveniments de seguretat de la informació.	10%	L1
	A.16.1.3	Notificació dels punts dèbils de la seguretat.	50%	L2
	A.16.1.4	Valoració dels esdeveniments de seguretat de la informació i pressa de decisions.	50%	L2
	A.16.1.5	Resposta a els incidents de seguretat.	90%	L3
	A.16.1.6	Aprenentatge dels incidents de seguretat informàtica.	90%	L3
	A.16.1.7	Recopilació d'evidències.	50%	L2
A.17 Els aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci.			94%	L4
A.17.1 Continuïtat de la seguretat de la informació				
	A.17.1.1	Planificació de la continuïtat de la seguretat de la informació.	95%	L4
	A.17.1.2	Implantació de la continuïtat de la seguretat de la informació.	90%	L3
	A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	90%	L3
A.17.2 Redundàncies				
	A.17.2.1	Disponibilitat d'instal·lacions per el processament de la informació.	100%	L5
A.18 Compliment			66%	L2
A.18.1 Compliment dels requeriments legals i contractuals.				
	A.18.1.1	Identificació de la legislació aplicable.	0%	L0
	A.18.1.2	Drets de propietat intel·lectual (DPI).	50%	L2
	A.18.1.3	Protecció dels registres de l'organització.	100%	L5
	A.18.1.4	Protecció de dades i privacitat de la informació personal.	100%	L5
	A.18.1.5	Regulació dels controls criptogràfics.	95%	L4
A.18.2 Revisions de la seguretat de la informació.				
	A.18.2.1	Revisió independent de la seguretat de la informació.	0%	L0
	A.18.2.2	Compliment de les polítiques i normes de seguretat.	90%	L2
	A.18.2.3	Comprovació del compliment.	90%	L2

Resumint, en el següent gràfic podem veure com troba el compliment de manera global de la taula de controls de la ISO/IEC 27001:2013. Amb un 7% tenim una maduresa de nivell L0 i L1, amb un 12% tenim un L4, amb un 22% un L2, amb un 24% un L3 i amb un 27% un L5.



En la següent gràfica podem veure el nivell de compliment dels diferents dominis de la ISO/IEC 27003, els valors van de 0% al 100%. Cal dir que en aquest cas el nivell desitjat seria 100% o el més pròxim a aquest.



	Nivell de compliment
A.5 Política de Seguretat de la Informació	50%
A.6 Organització de la Seguretat de la Informació	26%
A.7 Seguretat dels Recursos humans	56%
A.8 Gestió d'actius	53%

A.9 Control d'accés	73%
A.10 Criptografia	95%
A.11 Seguretat física i de l'entorn	85%
A.12 Seguretat en les operacions	86%
A.13 Seguretat en les comunicacions	79%
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.	80%
A.15 Relació amb els proveïdors	60%
A.16 Gestió de incidències de seguretat de la informació	50%
A.17 Els aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci.	94%
A.18 Compliment	66%

Després de veure els dos gràfics anteriors i la taula resum del diferent dominis, podem dir que l'empresa Cotecom està aproximadament al 50% del compliment de la ISO 27002.

No Conformitats i observacions detectades

Tot seguit podem veure les principals no-conformitats majors (NCMajor) i menors (NCMenor) de les principals categories agrupades.

Nº No-Conformitat	NC01
Data	10/12/2014
Tipus	NCMajor
Descripció	Falten indicadors de compliment en la política de seguretat, ampliació de la documentació i la implantació de la millora continua.
CMM	L2
Domini de la Norma	5. Política de la seguretat de la informació
Acció correctiva	La política de seguretat és de recent creació i implantació, però requereix aprofundir més en la documentació, completar-la amb indicadors i un sistema de millora continua.

Nº No-Conformitat	NC02
Data	10/12/2014
Tipus	NCMajor
Descripció	A dia d'avui encara no s'han assignat les responsabilitats en matèria de seguretat i falta l'aprovació per part de direcció de la política de treball extern i confidencialitat.
CMM	L1
Domini de la Norma	6. Organització de la Seguretat de la Informació
Acció correctiva	Assignació de les responsabilitats en matèria de seguretat i esperar l'aprovació per part de la direcció de l'empresa de la política de treball extern i confidencialitat.

Nº No-Conformitat	NC04
Data	10/12/2014
Tipus	NCMajor
Descripció	Falta formació i conscienciació de la seguretat a nivell d'empresa i lloc de treball, no hi ha definits processos disciplinaris, falta definició en els processos de selecció, altes, baixes i canvi de lloc de treball.
CMM	L2
Domini de la Norma	A.7 Seguretat dels Recursos humans
Acció correctiva	Cal formar millor el personal en nivell de seguretat, cal assegurar que cada lloc de treball sap quines són les seves responsabilitats, definir processos disciplinaris i definir millor els processos de selecció, altes, baixes i canvi de lloc de treball.

Nº No-Conformitat	NC05
Data	10/12/2014
Tipus	NCMajor
Descripció	Tot i tenir un gestor documental i sistemes equivalents, hi ha molta informació que no està classificada de forma correcta, tampoc hi ha cap sistema de gestió de suports d'emmagatzematge.
CMM	L2
Domini de la Norma	A.8 Gestió d'actius
Acció correctiva	Cal verificar i classificar millor la informació de les unitats de xarxa samba, per altre banda valorar l'ús de suports d'emmagatzematge, i si cal o no una eina de control i xifrat d'aquests. Cal fer entendre a la organització la importància de la possible fuga o pèrdua d'informació.

Nº No-Conformitat	NC06
Data	10/12/2014
Tipus	NCMajor
Descripció	Cal millorar l'autenticació a informació confidencial, procediments segurs de inici de sessió en els equips de sobre taula, millora de les eines de administració i control de sistemes.
CMM	L2>L3
Domini de la Norma	A. 9 Control d'accés
Acció correctiva	Tot hi haver implantat un directori central d'usuaris, per a els serveis d'empresa cal implantar aquest sistema a l'entorn de treball per tal que l'accés als ordinadors dels treballadors també sigui segur, i realitzar una autenticació segura en els altres àmbits. Cal procedimentar millor i explicar l'inici de sessió pels usuaris finals. Des de Tic cal implantar eines d'administració que permetin millorar l'administració i control dels sistemes i la informació.

Nº No-Conformitat	NC07
Data	10/12/2014
Tipus	NCMenor
Descripció	Existeix una política que defineix l'ús de controls de xifrat i s'ha implantat un SSO
CMM	L4
Domini de la Norma	A.10 Criptografia
Acció correctiva	Es tenen les eines i està implantat en un 95% dels serveis de l'empresa, cal acabar d'implantar i documentar.

Nº No-Conformitat	NC07
Data	10/12/2014
Tipus	NCMenor
Descripció	Existeix una política que defineix l'ús de controls de xifrat i s'ha implantat un SSO
CMM	L4
Domini de la Norma	A.10 Criptografia
Acció correctiva	Es tenen les eines i està implantat en un 95% dels serveis de l'empresa, cal acabar d'implantar i documentar.

Nº No-Conformitat	NC08
Data	10/12/2014
Tipus	NCMenor
Descripció	Cal millorar la seguretat i controlar la sortida d'actius fora de l'Organització, i millorar les mesures per equips desatesos.
CMM	L3

Domini de la Norma	A.11 Seguretat física i de l'entorn
Acció correctiva	Buscar eines/aplicacions que permetin millorar la seguretat i control dels equips quan surten de l'organització. Millorar la política d'equips desatesos, amb protectors de pantalla o parada del sistema quan són hores de no treball.

Nº No-Conformitat	NC09
Data	10/12/2014
Tipus	NCMenor
Descripció	Restriccions en la instal·lació d'aplicacions i el registre d'activitats dels administradors i operadors de sistemes, no té tota la informació de canvis o modificacions.
CMM	L3
Domini de la Norma	A.12 Seguretat en les operacions
Acció correctiva	Limitar la instal·lació d'aplicacions, i millorar el registre d'activitats dels administradors i operadors de sistemes.

Nº No-Conformitat	NC10
Data	10/12/2014
Tipus	NCMenor
Descripció	Cal millorar la seguretat d'accés al servei de missatgeria electrònica, millorar la política i procediments d'intercanvi d'informació.
CMM	L3
Domini de la Norma	A.13 Seguretat en les comunicacions
Acció correctiva	Activació de l'autenticació amb dos passos per accedir al servei de missatgeria electrònica, actualitzar els procediments d'intercanvi d'informació i crear uns documents de conscienciació.

Nº No-Conformitat	NC11
Data	10/12/2014
Tipus	NCMenor
Descripció	Falta algun indicador, cal definir algun procés.
CMM	L3
Domini de la Norma	A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.
Acció correctiva	Revisar indicadors i processos.

Nº No-Conformitat	NC12
Data	10/12/2014
Tipus	MCMenor
Descripció	Política i clàusules incompletes.
CMM	L3
Domini de la Norma	A.15 Relació amb els proveïdors
Acció correctiva	Cal complimentar i actualitzar la política. Definir millor el tractament del risc dintre dels acords.

Nº No-Conformitat	NC11
Data	10/12/2014
Tipus	Hi ha un sistema bàsic de gestió d'incidències.
Descripció	MCMajor
CMM	L2
Domini de la Norma	A.16 Gestió d'incidències de seguretat de la informació.
Acció correctiva	Cal buscar o desenvolupar una eina que permeti la gestió de les incidències en la seguretat de la informació, ja que l'actual no compleix amb els

	requeriments marcats.

Nº No-Conformitat	NC11
Data	10/12/2014
Tipus	NCMenor
Descripció	Identificar la legislació aplicable i revisió independent de la seguretat de la informació.
CMM	L2
Domini de la Norma	A.18 Compliment
Acció correctiva	Cal revisar la legislació aplicable i mirar que tot estigui al dia, acordar amb la direcció una auditoria externa del sistema de la informació cada 3 anys.

Conclusions

Després de finalitzar l'auditoria de compliment ISO/IEC 27002:2013 observem que la organització ha experimentat una important millora en el que es refereix a termes de seguretat de la informació respecte la seva situació inicial, on era pràcticament inexistent en relació a la situació actual. Tot i que en aquesta primera auditoria encara han aparegut dominis amb nivells de maduresa molt baixos, en els que cal seguir treballant i analitzant per tal d'obtenir millora.

També cal dir que els valors obtinguts són estimats ja que només s'han fet en funció dels projectes presentats en aquesta memòria i a dia d'avui no s'han implantat. Estan en previsió d'implantació un cop s'hagin aprovat els pressupostos del proper any.

Tal com s'ha dit abans, un 27% es manté en nivells de maduresa L5, un 12% en L4, un 24% en L3, un 22% a L2 i en un 14% L0 i L1.

Aquestes dades demostren que a dia d'avui estem aproximadament a un 30% del compliment de la ISO. També cal acotar amb més detall quins són els objectius en matèries de la seguretat de la informació que té l'empresa, per així poder acostar-ho el màxim possible a la realitat de l'organització.

Recuperant la taula del nivell de compliment, podem veure quina és la situació dels controls per dominis, on cal remarcar la manca d'organització de la seguretat de la informació, la política de seguretat, la gestió de les seves incidències i la gestió d'actius, per això cal revisar i solucionar les seves no conformitats.

	Nivell de compliment
A.5 Política de Seguretat de la Informació	50%
A.6 Organització de la Seguretat de la Informació	26%
A.7 Seguretat dels Recursos humans	56%
A.8 Gestió d'actius	53%
A.9 Control d'accés	73%
A.10 Criptografia	95%
A.11 Seguretat física i de l'entorn	85%
A.12 Seguretat en les operacions	86%
A.13 Seguretat en les comunicacions	79%
A.14 Adquisició, desenvolupament i manteniment dels sistemes d'informació.	80%
A.15 Relació amb els proveïdors	60%
A.16 Gestió de incidències de seguretat de la informació	50%
A.17 Els aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci.	94%
A.18 Compliment	66%

Per acabar podem dir que mitjançant l'elaboració d'aquest projecte s'ha pogut observar la situació de Cotecom, amb els diferents riscos i amenaces als que es troba exposat i ha permès començar a establir les guies que marcaran el futur del seu Sistema de Gestió de la Seguretat de la Informació.

Bibliografia:

ISO27001
http://www.iso27000.es

Margerit i anàlisi de risc
www.securityartwor.es
http://www.securityartwork.es/2012/04/24/analisis-de-riesgos-con-magerit-en-el-ens-i/
http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

PAE – Portal administració electrònica
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VH9LC4t9rKM

Inteco – Actius MARGERIT
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_07.swf
Inteco – SGSI
www.inteco.es

Apunts assignatura : Sistema de Gestió de la seguretat de la informació – UOC