Màster Interuniversitari en Seguretat de les TIC

(MISTIC)

TREBALL FINAL DE MASTER

Pla Director de Seguretat

NUCSSION

Alumne: Enrique Rubio Rodríguez

DNI: 46.320.965-T

Juny 2012

Index de continguts

Index d'il·lustracions

Index de Taules

1-Resum executiu

1.1-Introducció

NUCSSION desenvolupa la activitat de producció de energia elèctrica, mitjançant la fissió. Aquest procés es dut a terme amb elevats nivells de sofisticació i contemplant la seguretat, com element prioritari.

D'altra banda, NUCSSION, es una infraestructura crítica que en el cas de patir un atac, causaria gran impacte sobre la seguretat, tant física com econòmica dels ciutadans o sobre el bon funcionament del Gobern.

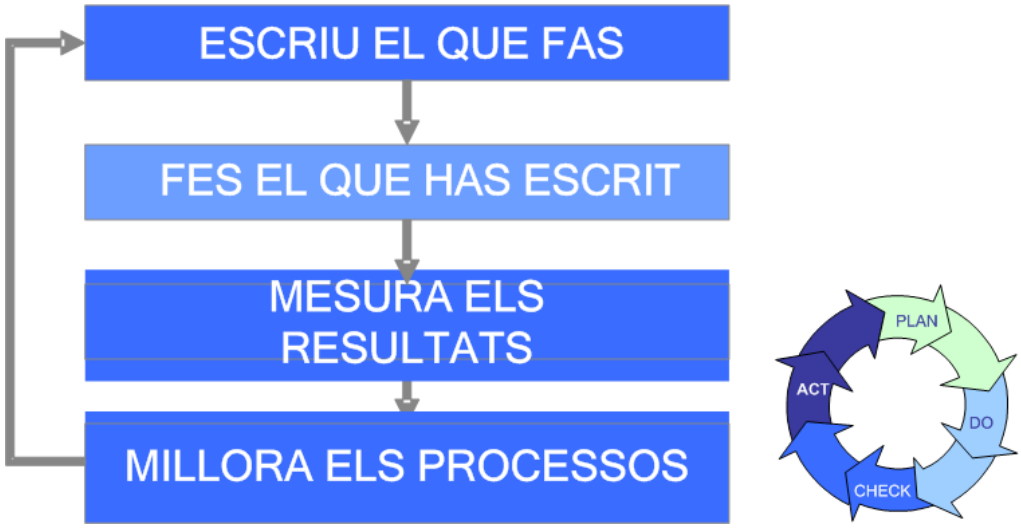
Actualment, els sistemes que controlen les infraestructures crítiques estan connectats amb xarxes de gestió, xarxes d'usuaris i, inclús, amb Internet. Per tant, el risc de que es materialitzi un incident en aquest tipus d'infraestructures es cada cop mes gran.

NUCSSION, conscient d'aquesta problemàtica, ha considerat fer una anàlisi objectiu de la situació actual de la seguretat global, dels riscos i del potencial impacte pel negoci, per establir un criteris tècnics i unes directrius corporatives en matèria de seguretat, sustentades en un desenvolupament normatiu, que permetin incrementar els nivells de seguretat de la informació i que ajudin a assolir el compliment de les Lleis i normatives estatals i sectorials.

Com eina per dur a terme aquest objectius, la Direcció de TIC ha decidit elaborar aquest **Pla Director de Seguretat de la Informació**, utilitzant com a marc estàndard de referència la norma ISO/IEC 27001.

Aquest Pla Director ha permès, en base a una avaluació i anàlisi de riscos de seguretat de la informació, i la aplicació de les bones pràctiques definides a la norma ISO/IEC 27002:2005, obtenir un pla de projectes a executar, segons la criticitat i aportació de la disminució del risc, per tal d'incrementar els nivells de seguretat i de compliment, i integrar tot aquest proces dins del cicle de

millora continua (PDCA) en el que es basa la norma ISO/IEC 27001.



Il·lustració 1: Cicle de Deming (PDCA) estratègia millora continua

1.2-Fases del pla

El Pla director de Seguretat de la Informació de NUCSSION s'ha dividit en dos fases:

1. Fase inicial o de situació
2. Fase d'implantació de les accions de millora detectades a la fase inicial

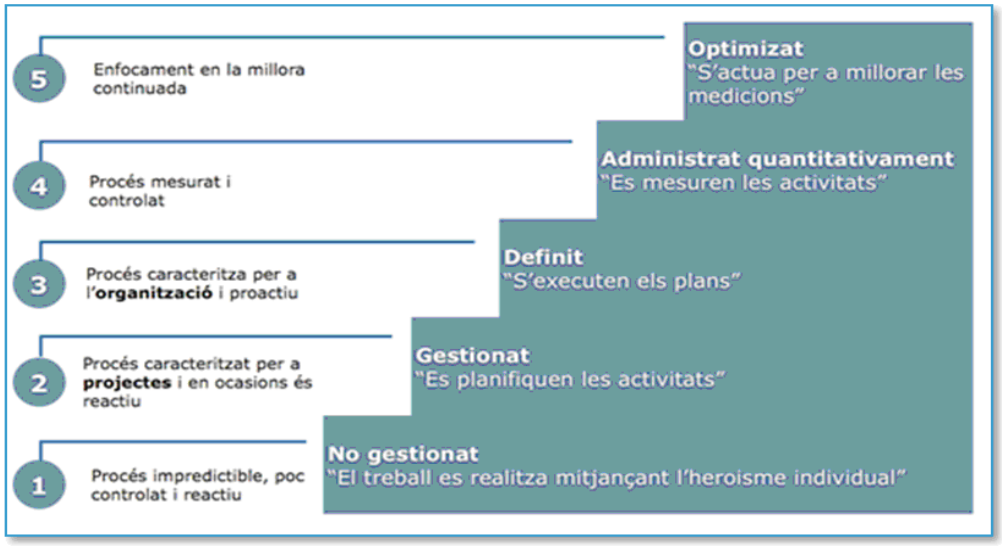
La fase inicial s'ha basat en la realització de l'anàlisi i avaluació de riscos. El resultat d'aquesta fase ha permès conèixer l'estat actual de la seguretat de la informació i identificar aquells aspectes que cal millorar.

Posteriorment, els aspectes de millora, han estat agrupats en projectes que s'han quantificat tant en esforç d'implantació com en cost econòmic.

Per dur a terme aquesta tasca s'ha utilitzat el Model de Maduresa de la Capacitat (CMM).

El **model CMM** [1] , es una col·lecció d'àrees de procés que contenen

metes i millors pràctiques que han de complir els processos de les organitzacions que el volen implementar. Existeixen dues “representacions” o maneres d’agrupar els processos. La més coneguda és l’esglaonada (*staged*) que agrupa les àrees de procés segons un “camí lògic” en l’increment de la maduresa en els processos de l’organització. És el que col·loquialment s’anomenen “els nivells CMM”.



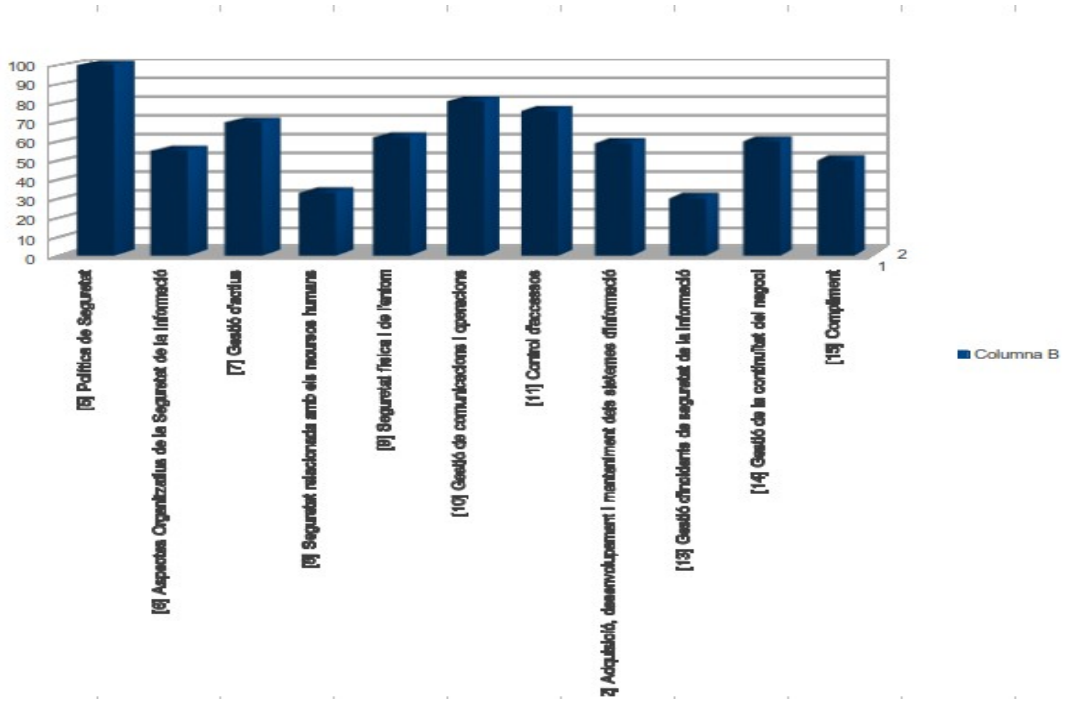
Il·lustració 2: Nivells CMM

Amb aquest model, i en base a criteris de compliment dels 133 controls de la ISO/IEC 27002:2005, s'ha obtingut el nivell de maduresa en el que es troba la seguretat en cada un dels onze dominis que defineix la norma.

Per situar cada domini en un determinat nivell de compliment, s'ha utilitzat la següent escala:

- Si el percentatge de compliment es 0% llavors Nivell CMM = L0
- Si el percentatge de compliment està entre 1% i 10% llavors Nivell CMM = L1
- Si el percentatge de compliment està entre 11% i 50% llavors Nivell CMM = L2
- Si el percentatge de compliment està entre 51% i 90% llavors Nivell CMM = L3
- Si el percentatge de compliment està entre 91% i 95% llavors Nivell CMM = L4
- Si el percentatge de compliment es mes gran el 95% llavors Nivell CMM = L5

El resultat d'aquesta fase ha revelat que el **nivell de compliment actual** es troba en un modest **61 %**, que segons l'escalat anterior el situaria a la part baixa de CMM3.



Il·lustració 3: Nivell actual de compliment per cada un dels onze dominis

Per augmentar el nivell de compliment, incrementat, conseqüentment, els nivells de seguretat i de compliment legal i normatiu, el Pla Director de Seguretat de la Informació de NUCCSION, ha desenvolupat un Pla de Projectes o Pla d'acció a tres anys.

Amb aquest Pla de Projectes, es pretén, durant el primer any, implantar aquelles accions correctores de menys cost i que comporten un esforç menor. La implantació d'aquestes accions permetrà incrementar el nivell de compliment fins CMM3 per tots els dominis de seguretat, assolint un nivell de compliment mínim del 80%.

Dintre dels dos anys següents, s'implantaran aquelles accions que representin un esforç mes alt o que tinguin un major impacte econòmic.

L'objectiu que es pretén **aconseguir**, quant s'hagin implantat tots els projectes es apropar el nivell de compliment a **CMM5, amb un nivell de compliment percentual del 95%**

El procés de millora continua garanteix que, després del desplegament inicial, un cop implantats tots els projectes, en base a les revisions periòdiques, es produirà una re alimentació que permetrà anar afinat i mantenint aquest CMM5 proper al 95%.

1.3-Resum de projectes

ID	Descripció	Cost	Esforç
P1	Ampliació de la Política de Seguretat i dels marcs contractuals	30.000€	7 mesos
P2	Millora de la Seguretat Física a les zones d'accés restringit i a les zones de carrega i descarrega	2.000€	2 mesos
P3	Gestió dels drets d'accés	40.000€	6 mesos
P4	Prevenció de l'us indegut dels recursos de tractament de la informació	40.000€	8 mesos
P5	Millora de les polítiques de seguretat	50.000€	12 mesos
P6	Millora de la seguretat del CPD, dels suports (backups i ordinadors portàtils)	34.500€	12 mesos
P7	Millora de la seguretat del software comercial o el desenvolupat a mida	60.000€	12 mesos
P8	Millora entorn desenvolupament NUCSSION	5.000€	6 mesos
P9	Aïllament físic de les xarxes de gestió i procés	90.000€	24 mesos

Tabla 1: Resum de Projectes

El pla de projectes s'ha dividit en nou projectes que agrupen un total de 37 accions correctores, amb un esforç de tres anys i uns costos de 351.000€

1.4-Conclusions

Com es veurà al desenvolupament del pla, l'objectiu de apropar al nivell CMM5 totes les dimensions de la seguretat, encara que en el decurs del temps serà factible, no s'aconseguirà del tor. Encara queda un camí per recórrer a la recerca de l'excel·lència.

Aquest camí s'haurà d'anar assolint mitjançant un proces de millora continua (PDCA) basat en la revisió periòdica del Pla o cada vegada que s'implanti un canvi significatiu.

L'èxit fonamental d'aplicació d'aquest Pla director, serà, l'increment notable del nivell de seguretat dels sistemes d'informació de NUCSSION i el compliment exigit pel regulador (CSN) quant a la implantació d'una política de defensa en profunditat basada en la utilització de dispositius unidireccionals.

Finalment, l'esforç total, serà de tres anys i 351.500€. Cal recordar que una sanció per incompliment greu de LOPD pot anar de 300.000 a 500.000€ amb el que la inversió, que no només millora el compliment LOPD, sinó que alinea la seguretat de les TI amb el negoci, es pot considerar que ha estat mes que raonable.

2-Seguretat de la Informació

2.1-Introducció

La informació i els sistemes que la suporten són l'actiu mes important pel desenvolupament de qualsevol activitat empresarial.

Els avenços tecnològics, l'accés massiu a Internet o els usuaris amb informació i formació insuficients, han contribuït a generar noves amenaces i vulnerabilitats per els sistemes d'informació.

Sovint, les conseqüències d'un incident de seguretat són importants, fet que ha provocat que la difusió de notícies relacionades amb la seguretat informàtica hagi transcendit dels àmbits tècnics i sigui freqüent a la premsa i, per tant, motiu de tractament social.

Un incident de seguretat informàtica es un esdeveniment advers en què algun aspecte de la seguretat de la informació està amenaçat, per exemple: la pèrdua de confidencialitat de les dades, interrupcions del sistema, interrupció o denegació de serveis, etc.

Alguns exemples poden ser: l'esborrat no autoritzat o accidental d'un arxiu; caigudes en el subministrament elèctric; trucades telefòniques o correus electrònics on s'intercanvien contrasenyes; atacs per virus i similars; intrusions en els sistemes per part de persones no autoritzades; etc. Per altra banda, depenent del efectes que puguin tenir per a l'empresa, els incidents solen classificar-se d'acord amb les següents categories:

- **Integritat compromesa**: com quan un virus altera un programa, informa un usuari extern de vulnerabilitats en un sistema, corromp arxius, etc.
- **Denegació de servei**: com quan un volum inusual de consultes a una plana web satura els servidors i no permet que cap usuari pugui veure la plana
- **Abús**: com quan un empleat realitza un ús no autoritzat d'un compte d'usuari o uns privilegis que no li pertoquen
- **Danys**: com quan un virus esborra arxius
- **Intrusions**: com quan un usuari extern penetra en els sistemes de l'empresa

Tots aquests incidents poden produir-se tant per causes externes com per causes internes, fet que comporta la necessitat d'una visió integral de la seguretat.

2.2-Amenaces externes

Una amenaça externa pot provindre d'un atac a través d'Internet per robar secrets de l'empresa, per manipular el funcionament de determinats sistemes, per cercar reconeixement dintre de certs cèrcols tècnics (fenomen **hacker**), repte intel·lectual, etc.

D'altra banda, donada la globalitat d'Internet, la quantitat d'usuaris malintencionats a la xarxa no és menyspreable.

Tot plegat provoca casos freqüents de diversos fenòmens, com ara atacs de virus informàtics i similars. Els virus poden destruir dades emmagatzemades ala sistemes d'informació empresarial, encara que també hi ha virus no destructius que únicament molesten l'usuari. Les formes en què un sistema es pot infectar són variades, però algunes de les mes freqüents son:

- Missatges que executen programes automàticament (com el programa de correu electrònic que obre directament un arxiu adjunt)
- Missatges que ens conviden a executar un programa adjunt per tal d'optar a un premi
- Intercanvi de fitxers a través dels programes de missatgeria instantània o peer-to-peer
- Inserció d'altres tipus de malware a partir de la visita a planes web, per exemple.

2.3-Amenaces internes

Bona part de les amenaces externes es materialitzen en incidents de seguretat a causa d'actuacions poc curoses o simple desconeixement dels usuaris.

De fet, els propis usuaris juntament amb la manca de procediments d'ús dels sistemes i la manca de polítiques de seguretat configuren el més alt

nombre d'incidents. Per exemple: els accessos no autoritzats a la informació; la pèrdua de dades per negligència; intercanvi de disquets, discs removibles o claus USB d'usuaris infectats; instal·lació de programari pirata; o tots els incidents derivats de l'anomenada enginyeria social.

Cal tenir present l'especial incidència, que en empreses com NUCSSION, ha tingut el cuc **Stuxnet.** L'**atac** s'ha **centrat sobre les plantes nuclears** (especialment iranianes) i **centrifugadores d'urani** controlades per **PLCs PCS7 de SIEMENS**. La via de contagi ha estat la inserció d'un dispositiu USB a un ordinador connectat directament a la xarxa de PLCs o de control de planta.

L'enginyeria social es basa en obtenir informació confidencial manipulant els seus usuaris legítims. Un "enginyer social" utilitzarà Internet o el telèfon per enganyar les seves víctimes. Pretén que li revelin informació confidencial o facin alguna cosa fora de la llei per al seu interès. Amb això s'explota la tendència natural de moltes persones a creure's la paraula de "l'enginyer" més que no pas explotar les possibles vulnerabilitats informàtiques que poguessin existir a l'ordinador de la víctima.

Generalment es considera que els usuaris són "l'esglaó més feble" dintre dels esquemes de seguretat, i per això és possible l'enginyeria social.

Tot plegat són fets potencials (externs o interns) que amenacen la seguretat d'un dels actius més importats de tota organització: les seves dades. Així doncs, quan es tracta la problemàtica de la seguretat és **precís tractar aspectes més enllà dels merament tècnics**: la disponibilitat de les dades; el manteniment dels ordinadors personals, els servidors i les xarxes; els tallafocs i antivirus; etc. Cal una visió global on es tinguin en compte, a més, aspectes com la integritat i la confidencialitat de la informació. És a dir, aspectes directament relacionats amb la gestió i l'operativa de l'empresa, així com la legalitat vigent.

Addicionalment, la norma l**SO / IEC 27000**, que és un conjunt d'estàndards desenvolupats o en fase de desenvolupament per *ISO (International Organization for Standardization) i IEC (International Electrotechnical Commission)*, **proporcionen una guia de bones pràctiques i un marc de gestió de la seguretat de la informació** utilitzable per qualsevol tipus de organització, pública o privada, gran o petita.

2.4-Objectius de la gestió de la seguretat de la informació

La gestió de la seguretat de la informació no tracta d'aconseguir l'absència de vulnerabilitats i d'incidents, cosa molt poc probable. Al contrari, tracta de generar confiança pel fet de saber que els possibles incidents estan sota control. És a dir, s'estudien les vulnerabilitats i es coneixen els potencials incidents, s'avalua el risc i es calcula l'impacte que tindrien en l'empresa, per finalment dissenyar un pla d'actuacions en cas que un incident acabi succeint. Aquest enfocament preventiu de la seguretat contrasta amb el de la seguretat reactiva, que es basa en la suposició que "no ha de passar res". Per tant, pretén un fals estalvi de costos mentre "no passa res", però queda a expenses del que realment acabi succeint si finalment "passa alguna cossa".

En aquests casos sol ser necessari recórrer a professionals altament qualificats en informàtica forense per tal que intentin recuperar alguna informació, seguir la pista de quin usuari ha actuat de mala fe, descobrir l'origen d'un atac, etc. Al marge que aquests serveis són certament costosos, no cal dir que la probabilitat d'èxit és relativa i que, potser, ja és massa tard per trobar solucions.

2.5-Avantatges de la gestió de la seguretat de la informació

Els avantatges de seguir el camí de la seguretat preventiva són variats depenent del grau d'implantació de les mesures de seguretat. En tot cas, es pot dir que en general es millorarà en tots o alguns dels següents aspectes:

- Integritat de la informació i els seus sistemes de suport
- Protecció d'un dels actius més importants de l'empresa: les dades
- Protecció d'informació sensible i/o subjecta a regulacions com la **LOPD**,

normativa CSN, **CNPIC**, **NRC**, **NUREG,** etc., per evitar sancions i garantir-ne el compliment

- Increment de la qualitat en la gestió del sistemes i les dades, millorant servei als usuaris
- Estalvi de temps i diners en cas d'incident, garantint de continuïtat del negoci

Finalment, cal remarcar que una gestió adient de la seguretat de la informació i els seus sistemes de suport contribuirà a disminuir els riscos que suporta l'empresa i a minimitzar el dany en els actius d'informació i coneixement, en cas que algun dels riscos acabi materialitzant-se.

2.6-Costos de la seguretat de la informació

Amb l'ampli ventall d'àmbits d'actuació per potenciar la seguretat dels sistemes i les dades, la inversió pot ser molt variable en funció de quin sigui el punt de partida, quins siguin els requeriments de seguretat, quins riscos es poden assumir i quins no, etc.

Cal tenir en compte que la seguretat no és un fi en si mateix, sinó que és tracta d'un procés més de l'organització. La necessària integració amb la resta de processos requerirà d'i**nversió en temps dels treballadors** fins que s'assumeixi el procés, **compromís de la direcció** per impulsar les mesures i fer arribar els beneficis a la resta de treballadors, etc. A més, com tot procés, la seguretat és quelcom "viu" (noves amenaces, continua evolució tecnològica, etc.) i s'haurà de mantenir i actualitzar periòdicament.

3-Descripció de l'empresa

3.1-Introducció

La empresa per a la que es desenvoluparà aquest Pla Director de Seguretat pertany al sector industrial de generació d'energia elèctrica.

La empresa disposa d'una planta de generació d'energia elèctrica capaç de produir fins a 500 MW/h, basada en el primer reactor de fusió instal·lat a Catalunya. Aquesta nova tecnologia permet que la instal·lació industrial sigui d'una mida reduïda i el seu disseny permet ubicar la planta aprop del nucli de població o industrial que requereix la energia elèctrica.

Per tal de controlar tot el proces de producció d'energia, la planta disposa d'un **ordinador digital de processos (ODP) que controla i registra les dades subministrades pels PLCs de camp**. Aquest ordinador es un element bàsic pel funcionament de la planta i en cas de no estar disponible, la planta ha d'aturar el seu proces de generació d'energia elèctrica.

Els PLC interactuen amb la instrumentació de la planta i les **comunicacions entre PLCs e instruments** es realitza, en tots els casos, **mitjançant BUS d'instrumentació GPIB**. Cada instrument esta connectat a dos PLCs mitjançant aquest BUS. Sempre ha d'haver, com a mínim, un PLC en servei per a cada instrument de la planta.

Tots els PLCs estan connectats al ordinador de processos (ODP) mitjançant una xarxa Ethernet.

L'ODP, que es troba situat en un CPD dintre del edifici de control, disposa de vint (20) de terminals de consulta repartits entre la sala de control i els edificis mes rellevants com per exemple l'edifici de turbines. D'altra banda, l'ODP disposa de dos panells de visualització en temps real del estat de la planta. En aquests panells es poden veure les alarmes produïdes pel mal funcionament d'un instrument o d'un PLC, així com l'estat de producció d'energia elèctrica. Els panells son redundants i, com a mínim, un panell ha de estar en funcionament per que la planta pugi funcionar.

D'altre banda, la empresa disposa d'un **departament TIC** que amb les seves infraestructures (servidors, storage, xarxes de comunicació de veu i dades, connectivitat amb l'exterior, estacions de treball d'usuaris, etc.), proporcionen serveis de **Gestió Tècnica** com ara, la planificació del manteniment preventiu,correctiu i evolutiu dels components de la planta, la gestió d'ordres de treball, la gestió de permisos de treball, la nòmina dels empleats, la Intranet corporativa, gestió de recanvis i materials, gestió del magatzem, etc. Departaments com Enginyeria, Manteniment, RRHH, Comptabilitat, Magatzem, etc., utilitzen les infraestructures TIC per desenvolupar les seves tasques: Disseny i dibuix de plànols, especificacions de càlculs d'obra civil, catàlegs d'elements, etc.

El parc d'estacions de treball es de 200 i estan distribuïdes per tota la planta. Cada usuari d'aquestes estacions de treball disposa del seu identificador i contrasenya personals per accedir al sistema, i ho pot fer des-de qualsevol de les estacions de treball.

Totes les estacions de treball es troben connectades en xarxa. La xarxa està segmentada per edificis. Cada edifici disposa d'un switch (diferent del de l'ODP) i cada switch es connecta mitjançant FO amb el “core” de TIC, ubicat en el CPD de TIC.

Tots els usuaris tenen accés lliure a Internet, si be existeix un proxy que s'encarrega de filtrar continguts de dubtosa reputació.

Alguns usuaris, per dur a terme la seva tasca, necessiten obtenir informació de l'ODP. Per poder accedir a la informació de l'ODP, necessiten disposar d'un perfil d'usuari que permeti executar aplicacions que puguin fer peticions a uns frontends situat a la xarxa ODP.

Entre la xarxa TIC i la xarxa ODP existeix un Firewall controlat per explotació SDP que permet, en determinades circumstàncies, una comunicació entre ambdues xarxes.

Alguns directius, caps de servei i administradors de sistemes, tenen la

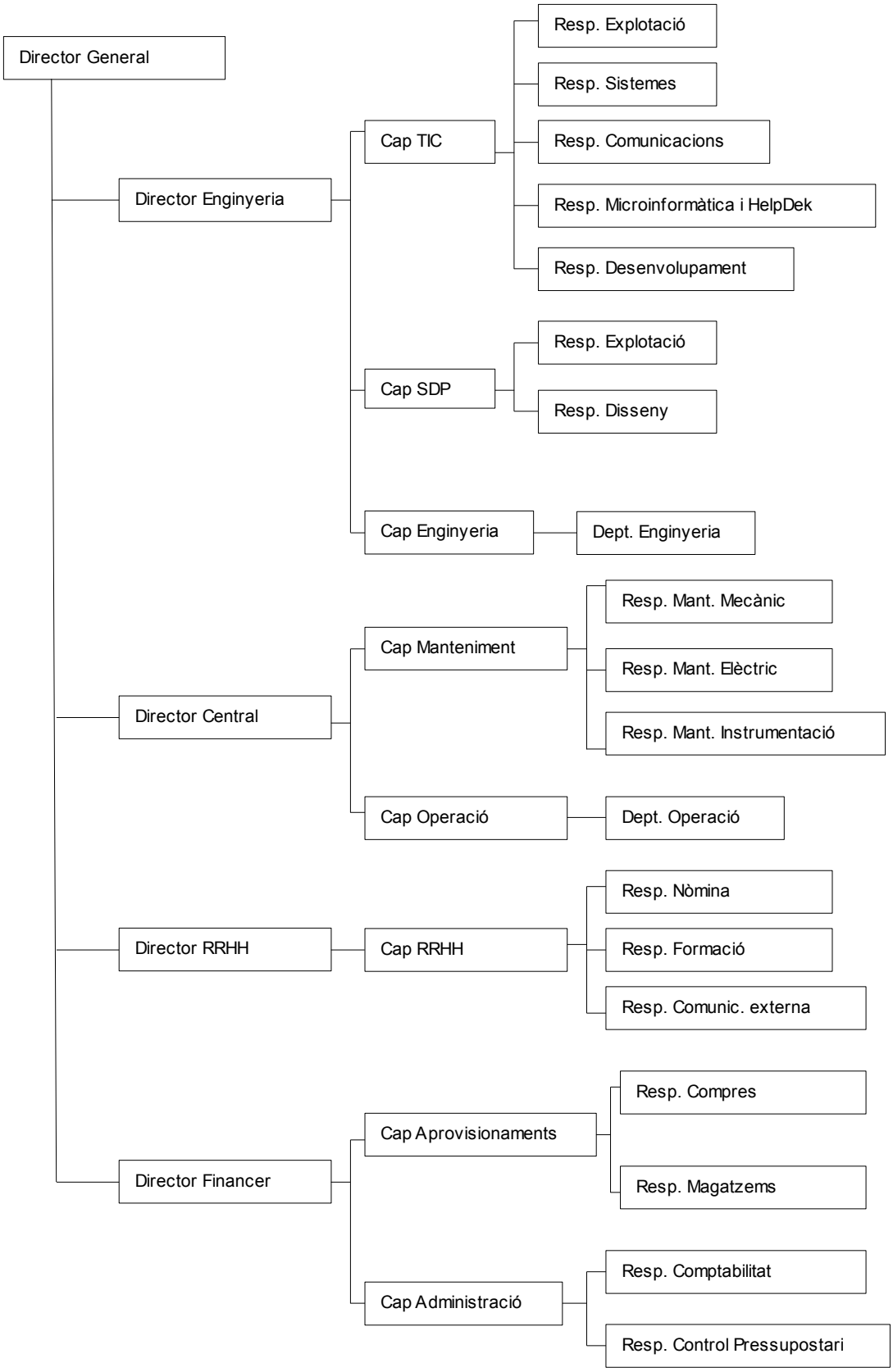
possibilitat d'accedir des-de casa seva al sistema. Son un petit grup d'usuaris autoritzats i controlats que accedeixen a un portal captiu que els sol·licita un usuari + password i una autenticació forta proporcionada per un token personal RSA.

Tant els servidors com las cabines d'storage, estan en altres segments de la xarxa a on els usuaris, directament des-de les seves WS no hi poden arribar

Tots els usuaris disposen d'un espai de xarxa (disc de xarxa) personal i privar per guardar els seus documents. Per polítiques de seguretat es recomana als usuaris que no guardin arxius importats als seus PCs i que ho facin el disc de xarxa.

Totes les WS disposen d'antivirus actualitzat.

3.2-Organigrama



3.3-Distribució de la plantilla

3.3.1-Direcció

Un director General i quatre Directors d'Àrea.

3.3.2-Àrea d'Enginyeria

Esta formada per tres subàrees que es distribueixen de la següent forma:

3.3.2.1-TIC Tecnologies d'Informació i Comunicacions (36) persones

Exploten, administren i evolucionen tant el hardware com el software del sistemes TIC de suport a les activitats de negoci de la empresa.

- Cap d'àrea TIC: Cap d'àrea
- Explotació: Cap d'explotació i 9 tècnics
- Sistemes: Cap de sistemes i 3 tècnics.
- Comunicacions: Cap de comunicacions i 4 tècnics
- Microinformàtica i HelpDesk: Cap de microinformàtica, 3 tècnics HW i 2 operadors de helpdesk.
- Desenvolupament: Cap de desenvolupament i 9 enginyers.

3.3.2.2-SDP Sistemes Digitals de Proces (10) persones

Exploten i administren l'ordinador de proces (ODP) i fan el disseny i seguiment de la implantació de les modificacions que afecten a tot el sistema SCADA de la planta.

- Cap d'àrea SDP: Cap d'àrea.
- Explotació: Cap d'explotació i 4 tècnics.
- Disseny: Cap de disseny i 3 enginyers.

3.3.2.3-Enginyeria (39) persones

Realitzen les tasques de disseny corresponents als canvis de disseny de la planta i supervisen el correcte funcionament de la planta. Cada enginyer es responsable d'un numero determinat de sistemes de la planta.

- Cap d'àrea d'enginyeria: cap d'àrea.
- Departament enginyeria: 38 enginyers

3.3.3-Àrea de direcció de Central

Esta formada per dos subàrees que es distribueixen de la següent forma:

3.3.4-Manteniment (49) persones

Duen a terme les tasques de manteniment preventiu, correctiu i evolutiu dels elements que composen la planta.

- Cap d'àrea MTO: Cap d'àrea

Aquesta subàrea esta dividida en tres especialitats:

3.3.4.1-MEC Manteniment Mecànic:

S'ocupen dels elements mecànics que conformen la planta com ara: tubàries, vàlvules, suports, equips d'aire condicionat (AAC), motors dièsel d'emergència, etc.

- Cap d'especialitat MEC: Cap d'especialitat i 15 mecànics.

3.3.4.2-ELC Manteniment Elèctric:

S'ocupen dels elements elèctrics que conformen la planta com ara: cablejat d'alta i baixa tensió, quadres d'interconnexió, accionadors elèctrics de vàlvules i d'altres elements que requereixin accionament o alimentació elèctrica.

- Cap d'especialitat ELC: Cap d'especialitat i 15 electricistes.

3.3.4.3-INS Manteniment Instrumentació:

S'ocupen dels instruments i dels seus llaços de connexió (bus GPIB entre d'altres). Els instruments poden estar ubicats tant a la sala de control com a camp i poden ser de diversos tipus: PLCs, sondes, sensors, lectores de dosímetres, etc.

- Cap d'especialitat INS: Cap d'especialitat i 15 instrumentistes.

3.3.5-Operació (36) persones

S'ocupen de les tasques de supervisió, control i operació de la planta. Al ser un torn tancat de 24x7, existeixen 7 grups o torns, de cinc persones que van rotant segons un quadrant de torns. En condicions normals, sempre estan tres torns operatius (matí, tarde i nit), un torn de reten, un torn en formació i dos torns descansant.

- Cap d'operació OPE: Cap d'operació.
- Per cada torn: Un cap de torn i 4 operadors

3.3.6-Àrea de Recursos Humans

Esta formada per tres subàrees que es distribueixen de la següent forma:

- Cap d'àrea RRHH: Cap d'àrea

Nomines (3) persones

Son els responsables de confeccionar la nomina de tota la plantilla, aplicant tant la normativa vigent derivada del corresponent conveni col·lectiu, com la derivada de la legislació vigent.

- Responsable de nomines i 2 administratius tècnics de nomines.

Formació (11) persones

Es l'àrea responsable de supervisar e impartir tant la formació per empleats recent incorporats a la empresa com de fer el entrenament anual per tot el personal.

- Responsable de formació i 10 formadors.

Comunicació externa (4) persones

Son els responsables de transmetre la informació corporativa tan internament com al exterior de la empresa.

- Responsable de comunicació, 1 enginyer i 2 periodistes.

3.3.7-Àrea de Finances

Esta formada per dos subàrees que es distribueixen de la següent forma:

Aprovisionaments (14) persones

El l'àrea encarregada de que la planta sempre disposi dels recanvis, materials i serveis de personal extern que pugui necessitar per desenvolupar el negoci.

- Cap d'àrea APR: Cap d'àrea

Aquest àrea es divideix en dos subàrees:

3.3.7.1-*Compres*.

La forma un grup d'agents de compres especialitzats en materials i recanvis o en serveis. Quan un departament te la necessitat d'adquirir un be (tan sigui un material com un servei), aquest departament inicia un proces de selecció del proveïdor mes adient per contractar el servei o comprar el material.

- Cap de compres i 5 agents de compres

3.3.7.2-Magatzems

Esta format per un grup de magatzemers que es cuiden de ubicar en les condicions requerides tots els recanvis i de subministrar-los als departaments de manteniment que els requereixin per realitzar la seva tasca.

- Cap de magatzems i 6 magatzemers.

3.3.8-Administració (12) persones

El l'àrea encarregada dels temes fiscals, pressupostaris i comptables.

- Cap d'àrea ADM: Cap d'àrea

Aquest àrea es divideix en dos subàrees:

3.3.8.1-Comptabilitat

S'encarrega de dur la comptabilitat de la empresa d'acord amb la normativa vigent. També s'encarreguen de la tresoreria, el control de bancs i de controlar les factures del proveïdors, així com d'ordenar el pagament d'aquestes quan han estan conformades. Son també els encarregats d'ordenar el pagament de les nòmines d'empleats.

- Responsable de Comptabilitat, 2 comptables i 4 administratius.

3.3.8.2-Control Pressupostari

S'encarrega de fer el pressupost anual de despesa i inversió, així com de fer el seguiment del seu compliment.

- Responsable de control pressupostari i 3 administratius tècnics

3.4-Sistemes d'informació

3.4.1-Introducció

Per tal de complir amb la missió de la empresa, "*Operar la planta de forma segura i compromesa amb la seguretat de les persones i el medi ambient, garantint la producció a llarg termini*", els sistemes d'informació dels que disposa la planta es divideixen en dos grans grups.

D'una banda s'identifica el sistema d'informació involucrat directament amb el control físic de la planta, i que interactua amb els sistemes SCADA que la composen. Aquest sistema s'identifica amb el nom que rep l'ordinador de proces, **ODP.**

D'altra banda, s'identifica el sistema de Gestió Tècnica. Aquest sistema permet gestionar les tasques administratives i econòmiques de la empresa. Al sistema de Gestió Tècnica se l'anomene **GTEC.**

3.4.2-Sistema d'informació ODP

El nucli del sistema ODP està format per un ordinador de proces que rep i emmagatzema totes les senyals dels instruments de la planta i que, en base a la informació obtinguda, actua sobre alguns elements de la planta per modificar el seu comportament operatiu. Per exemple, quan l'ODP rep una senyal que indica que la planta ha quedat sense alimentació elèctrica exterior, inicia una serie de enviaments de ordres a certs PLCs de la planta per aturar el proces de producció.

3.4.2.1-Arquitectura física

Físicament, l'ODP està basat en un sistema redundant de quatre nodes tipus **blade** que es van repartint la carrega de recepció de senyals de la planta i que actuen enviant senyals de control als PLCs que mantenen la planta operativa.

Disposa de dos nodes més que s'encarreguen, únicament, de mostrar diagrames i alarmes en dos pantalles (videowalls) ubicades a la sals de control. Aquestes pantalles tenen connexió directe amb cada un dels nodes controladors.

L'ODP pot donar servei (en el mode de llicenciament actual) fins a 40 terminals de consulta. Aquest terminals son simples PCs que han de tenir instal·lat un programari subministrat pel fabricant i han d'estar connectats a la xarxa interna de l'ODP

Per subministrar informació a possibles peticions remotes, l'ODP disposa de de dos servidors forntend independents.

Quant als PLCs, son tots del tipus Siemens PCS7.

Tots els PLCs comuniquen amb els instruments dels que reben senyals i que controlen, mitjançant un bus d'instrumentació **GPIB** amb cablejat independent des del PLC al instrument.

3.4.2.2-Xarxa de comunicacions (Xarxa ODP)

Tots els element de l'ODP interactuen mitjançant una xarxa Ethernet. Aquesta xarxa te una segmentació física imposada per la distribució dels PLC i els terminals de consulta per tota la planta. Cada edifici disposa de dos **switchs CISCO 3550**. Un per connectar els terminals de consulta i l'altre per connectar els PLCs amb l'ODP. Cada switch comunica amb un **core CISCO 6550** en alta disponibilitat mitjançant una connexió punt a punt de Fibra Òptica.

La única excepció a aquesta comunicació Ethernet es la que mantenen els **PLC** i els **instruments** que es comuniquen entre ells amb **bus GPIB.**

El punt frontera de la Xarxa ODP, que permet, sota fortes mesures de seguretat, comunicar la xarxa interna de l'ODP amb la xarxa de Gestió Tècnica, es un Firewall Juniper SRX240 amb OS JUNOS 10.3 (**Firewall ODP**)

3.4.2.3-Software

El sistema operatiu que corre en cada node de l'ODP es Windows Server 2008-R2 de 64 bits.

El sistema operatiu dels frontends es windows Server 2008-R2 de 64 bits amb un IIS 7 com a servidor web que respon a les peticions remotes. L'IIS interactua amb un programari tancat subministrat pel fabricant que es el que accedeix a les dades del ODP i els hi dona format per la seva resposta al

peticionari.

Els PLC fan servir OS Windows i programació WinCC.

El sistema operatiu dels terminals connectats a l'ODP por ser Windows XP SP3 o Windows 7 Professional

El programari del ODP per realitzar la captura de senyals i de actuació dels PLCs es un paquet tancat subministrat pel fabricant del sistema. Aquest programari permet, al **personal format com administrador del sistema**, realitzar les següents tasques:

- Afegir nous terminals al sistema (explicitant la adreça IP amb la que han estat instal·lats), fins el màxim de llicencies.
- Afegir/eliminar usuaris al sistema. Cada usuari ha de tenir una combinació usuari/password per poder accedir en mode consulta des-de qualsevol terminal connectar a l'ODP.
- Realitzar els backups diaris del sistema , guardant-los al armari ignifug del CPD i traslladant la copia del dia anterior al segon armari ignifug fora del edifici.

3.4.2.4-Gestió i administració del sistema

L'administració del sistema, incloent les polítiques del firewall ODP i la configuració dels switchs i el core de la xarxa ODP, es responsabilitat de **explotació de SDP**.

Existeix un procediment per sol·licitar un **usuari/password** per accedir a l'ODP i altre per sol·licitar incloure un nou terminal al sistema. Ambdues sol·licituds han d'estar autoritzades pel Director d'Enginyeria.

3.4.2.5-Seguretat Física

Tot el nucli de l'ODP es troba en el CPD de SDP que es trobe ubicat al mateix edifici de control. El CPD de SDP disposa d'un control d'accés basat en una tarja magnètica i un PIN que només coneix el propietari de la tarja. Només poden accedir al CDP aquelles persones que disposin de la corresponent autorització atorgada en base a la sol·licitud corresponent que ha hagut de signar tant el Responsable d'explotació de SDP com el Director d'Enginyeria.

El CPD conta amb les mesures de seguretat següents:

- Control d'accessos personalitzat amb doble verificació (tarja+PIN)
- Sistema d'alimentació ininterrompuda on-line (SAI) que permet apagar ordenadament els sistemes en cas de perduda d'alimentació.
- Sistema d'aire condicionat.
- Sistema de detecció i extinció d'incendis automàtic.
- Armari ignifug per guardar les copies de backup diàries.

En un edifici pròxim, dintre del perímetre de seguretat de la planta, SDP disposa d'un segon armari ignifug mes gran a on es conserven les copies de seguretat diàries (del dia anterior),setmanals, mensuals i anuals.

3.4.3-Sistema d'informació GTEC

El sistema d'informació **GTEC** està format per una **aplicació modular** que permet dur a terme totes les tasques de caire administratiu que son necessàries en una planta industrial. Els mòduls mes rellevants, dels que se n'extreuen les principals funcionalitats son els següents:

- Catàleg d'Elements
  - Recull tots els elements que composen la planta per planificar les tasques de manteniment preventiu i correctiu.
- Planificació de Manteniment Preventiu
  - Genera les ordres de treball per realitzar el manteniment dels elements del catàleg en base a la data d'última execució i la freqüència de realització. A les ordres de treball es consignen les tasques a realitzar i síndica la llista de materials necessaris per realitzar la tasca de manteniment (recanvis a utilitzar, olis, eines, etc.)
- Sol·licitud de Manteniment Correctiu sobre un element (ST)
  - Genera una sola ordre de treball per realitzar una reparació d'un element del catàleg.
- Gestió d'Ordres de Treball (OT)
  - Gestiona i controla el flux de treball que genera una OT des-de la Apertura fins el Tancament.
- Gestió de Magatzem
  - Gestiona el magatzem de recanvis i/o materials pels elements del catàleg. Rep les comandes de recanvis i/o materials subministrats per proveïdors, ubicant els recanvis/materials dins el magatzem. Subministra materials als responsables de execució de les OT.
- Gestió de Compres
  - Gestiona les llistes de proveïdors. Emet peticions d'ofertes per adquirir materials o serveis als proveïdors de la llista. Compara ofertes i emet comandes de compra.
- Gestió de Personal
  - Manté la llista de treballadors, de plantilla i externs, que treballen o han treballat per la planta. Lliura les acreditacions que permet accedir als recintes de la planta.
- Formació
  - Manté els registres de la qualificació professional i de les titulacions de cada un dels treballadors. Manté els registres de re-entrenament anual de cada treballador.

- Nòmina
  - Gestiona el fitxer d'empleats de plantilla i confecciona la nòmina mensual.
- Comptabilitat
  - Realitza la gestió comptable, de tresoreria i de pagaments a proveïdors.
- Control Pressupostari
  - Confecciona el pressupost anual i en fa el seguiment del seu compliment.
- Gestió Documental
  - Registra i emmagatzema els diferents documents que utilitza la empresa: OTs tancades, Documentació d'Enginyeria, Planols, Procediments, Nòmines, etc.

A banda de GTEC, la empresa disposa d'una **Intranet** que es nodreix dels continguts de GTEC. Realment, la Intranet es un frontend que permet als usuaris cercar documentació, accedir al portal de l'empleat, llegir les noticies que publica el departament de comunicació Interna/Externa.

Finalment, la empresa disposa de una **Web corporativa**, accessible des-d'**Internet**, a on es publiquen dades d'interès general per a l'opinió pública. Aquesta **web corporativa** resideix en un **servei de hosting extern a la planta.**

3.4.3.1-Arquitectura física

La arquitectura física que dona suport a GTEC i a la Intranet corporativa, així com als serveis de correu electrònic, navegació d'Internet, accés remot, seguretat a l'end point i administració de la xarxa GTEC, es basa en els següents components:

- Servidor de BB.DD
  - Servidor d'alta disponibilitat, format per dos nodes BLADE BL680c G7 amb 256 Gb de RAM i 2 processadors Intel-Xeon X7550 de 8 nuclis, amb 6 ports FlexFabric NC5531i de 10 GbE. Cada Servidor compta amb dos discs SAS de 300 GB i 15000 RPM en RAID 1 per contenir el OS i el Gestor de BBDD.
- Servidor de Directori Actiu
  - Servidor d'alta disponibilitat, format per dos nodes BLADE BL 620c G7 amb 32 Gb de RAM i 1 processador Intel-Xeon E6510 de 4 nuclis,

amb 4 ports FlexFabric NC5531i de 10 GbE. Cada Servidor compta amb dos discs SAS de 300 GB i 15000 RPM en RAID 1 per contenir el OS.

- Servidor Web-IIS
  - Granja NLB format per quatre nodes BLADE BL 620c G7 amb 32 Gb de RAM i 1 processador Intel-Xeon E6510 de 4 nuclis, amb 4 ports FlexFabric NC5531i de 10 GbE. Cada Servidor compta amb dos discs SAS de 300 GB i 15000 RPM en RAID 1 per contenir el OS i el servidor IIS
- Servidor de fitxers
  - Granja NLB format per dos nodes BLADE BL 280c G6 amb 16 Gb de RAM i 1 processador Intel-Xeon E5506 de 4 nuclis, amb 2 ports 1GbE NC362i. Cada Servidor compta amb dos discs SAS de 15000 RPM en RAID 1 per contenir el OS.
- Servidor d'impressió
  - Granja NLB format per dos nodes BLADE BL 280c G6 amb 16 Gb de RAM i 1 processador Intel-Xeon E5506 de 4 nuclis, amb 2 ports 1GbE NC362i. Cada Servidor compta amb dos discs SAS de 15000 RPM en RAID 1 per contenir el OS.
- Servidor de Terminals per accessos remots d'usuaris
  - Granja NLB format per dos nodes BLADE BL 620c G7 amb 128 Gb de RAM i 1 processador Intel-Xeon E6510 de 4 nuclis, amb 4 ports FlexFabric NC5531i de 10 GbE. Cada Servidor compta amb dos discs SAS de 300 GB i 15000 RPM en RAID 1 per contenir el OS.
- Servidor de correu electrònic
  - Servidor BLADE BL 280c G6 amb 256 Gb de RAM i 1 processador Intel-Xeon E5506 de 4 nuclis, amb 2 ports 1GbE NC362i. El Servidor compta amb dos discs SAS de 15000 RPM en RAID 1 per contenir el OS i els servidors d'Exchange i antispam.
- Servidor Proxy
  - Servidor BLADE BL 280c G6 amb 64 Gb de RAM i 1 processador Intel-Xeon E5506 de 4 nuclis, amb 2 ports 1GbE NC362i. El Servidor compta amb dos discs SAS de 15000 RPM en RAID 1 per contenir el OS i el servidor proxy de WebSense.
- Secure Access Juniper SA2500
  - Appliance de Juniper Networks Terminador SSL i VPN per accessos remots.
- CISCO NAC APPLIANCE 3315
  - Appliance de CISCO per aplicar les polítiques d'accés a la XARXA

GTEC de les estacions de treball dels usuaris.

- Servidor de Terminals per Administració de comunicacions
  - Servidor BLADE BL 280c G6 amb 16 Gb de RAM i 1 processador Intel-Xeon E5506 de 4 nuclis, amb 2 ports 1GbE NC362i. El Servidor compta amb dos discs SAS de 15000 RPM en RAID 1 per contenir el OS i el SW d'administració de comunicacions.
- HP 4400 Enterprise Virtual Array (EVA)
  - Sistema d'storage en xarxa. Amb 80 Tb utils, 4 ports fibre Channel de 4Gb.
- Firewall Appliance Nokia IP560c
  - Firewall de perímetre amb SW CheckPoint
- Estació de treball d'usuari
  - PC amb 2 Gb de RAM, NIC 1Gb i HD 300Gb, USB+DVDRW

3.4.3.2-Xarxa de comunicacions (Xarxa GTEC)

Xarxa Ethernet amb una segmentació física imposada per la distribució de les estacions de treball per tota la planta. Cada edifici disposa de dos **switch CISCO 3550** per connectar les estacions de treball del usuaris i les impressores. Cada switch comunica amb un **core CISCO 6550** en alta disponibilitat mitjançant una connexió punt a punt de Fibra Òptica.

A banda d'aquesta segmentació imposada per la distribució de estacions de treball i impressores en edificis, la XARXA GTEC presenta la següent segmentació interna:

- Xarxa Externa o de Perímetre
  - Aquesta xarxa es la que interactua amb Internet. Disposa d'un Firewall Nokia amb Software CheckPoint que es la primera línia de defensa de la empresa amb l'exterior.
- Xarxa DMZ
  - Al darrera del FW de Perímetre, es situen les servidors que formen la DMZ. Aquest servidors son: el de correu, el proxy de sortida a Internet, el Secure Access per accessos des-de l'exterior. La xarxa DMZ es troba aïllada per un Firewall de sortida. Es a dir, la xarxa DMZ es troba entre el firewall del perímetre i el firewall de sortida.
- Xarxa de Servidors
  - Conté tots el servidors que donen servei a GTEC, i la cabina d'storage EVA 4400. Aquesta xarxa es troba aïllada de la xarxa d'usuaris pel corresponent firewall.
- Xarxa d'administració de comunicacions
  - Es una sub-xarxa de la xarxa d'usuaris. En aquesta xarxa es troba l'apliance NAC y el servidor de terminals que fa servir comunicacions per administrar els dispositius que composen la xarxa GTEC
- Xarxa d'usuaris
  - Es la xarxa a on se troben connectades totes les estacions de treball dels usuaris, les impressores i el Servidor de Terminals per accessos remots. Aquesta Xarxa es troba segmentada per edificis.

Tots els firewalls esmentats en aquesta xarxa, tret del firewall del perímetre son Juniper SRX240 amb OS JUNOS 10.3

3.4.3.3-Software

El sistema operatiu que corre en cada Servidor es Windows Server 2008-R2 de 64 bits.

El gestor de BB.DD que corre al servidor de BB.DD es SqlServer 2005

El servidor Web que corre al servidor Web-IIS es IIS-7

El software GTEC disposa d'una part que corre al servidor Web-IIS com a serveis Web. En aquest servidor també es troba instal·lat MicroSoft .Net framework 4.0

- Estacions de treball
  - El Sistema operatiu: Windows XP SP3 o Windows 7 professional.
  - Framework 4 de .NET
  - Navegador d'Internet: Iexplorer 7 / IExplorer 9
  - Antivirus McAfee (actualització diaria per ePO)
  - Accés directe, en mode lectura, al client GTEC (resident al servidor de fitxers)
  - Agent NAC de CISCO
  - Suite Microsoft Office 2010 incloent MSAccess
  - Microsoft Outlook i Microsoft Messenger for Outlook
  - Client de xarxa per SQLServer

3.4.3.4-Gestió i administració del sistema

L'administració i disseny del sistema, es distribueix entre els següents departaments de TIC:

- Sistemes
  - Realitza o avalua el disseny de totes les implantacions de sw/hw de TIC
- Comunicacions
  - Implanta i administra les polítiques dels firewalls i configuració dels switchs i el core de la xarxa GTEC, segon indicacions de sistemes.
- Explotació
  - Implanta i administra les polítiques del servidors, realitza els backups

del sistema d'arxius, de la BB.DD i de la cabina EVA diàriament, guardant-los al armari ignifug del CPD i traslladant la copia del dia anterior al segon armari ignifug fora del edifici.

- Administra els usuaris dels sistemes TIC:
  - Altes i baixes d'usuaris al directori actiu
  - Altes i baixes de comptes de correu electrònic
  - Assignació de perfils a usuaris per accedir a funcionalitats de GTEC o Intranet
- Les accions anterior requereixen petició explícita dels caps d'àrea de cada departament.
- Registra i controla tots els accessos al CPD de TIC.
- Implanta les modificacions i evolucions a la aplicació GTEC i la Intranet corporativa a petició del departament de Desenvolupament, mitjançant la recepció del corresponent traspas SW.

- Microinformática-Heplpdesk
  - Vetlla per la “salut” dels PCs d'usuari i del parc d'impressores.
  - Aten i registra, mitjançant telèfon d'atenció, les incidències d'usuari, intentant resoldre-les. En cas de no resolució, escalen la incidència al departament corresponent (Sistemes, Explotació, Desenvolupament)

3.4.3.5-Seguretat Física

El CPD de TIC disposa d'un control d'accés basat en una tarja magnètica i un PIN que només coneix el propietari de la tarja. Només poden accedir al CDP aquelles persones que disposin de la corresponent autorització atorgada en base a la sol·licitud corresponent que ha hagut de signar tant el Responsable d'explotació de TIC com el Director d'Enginyeria.

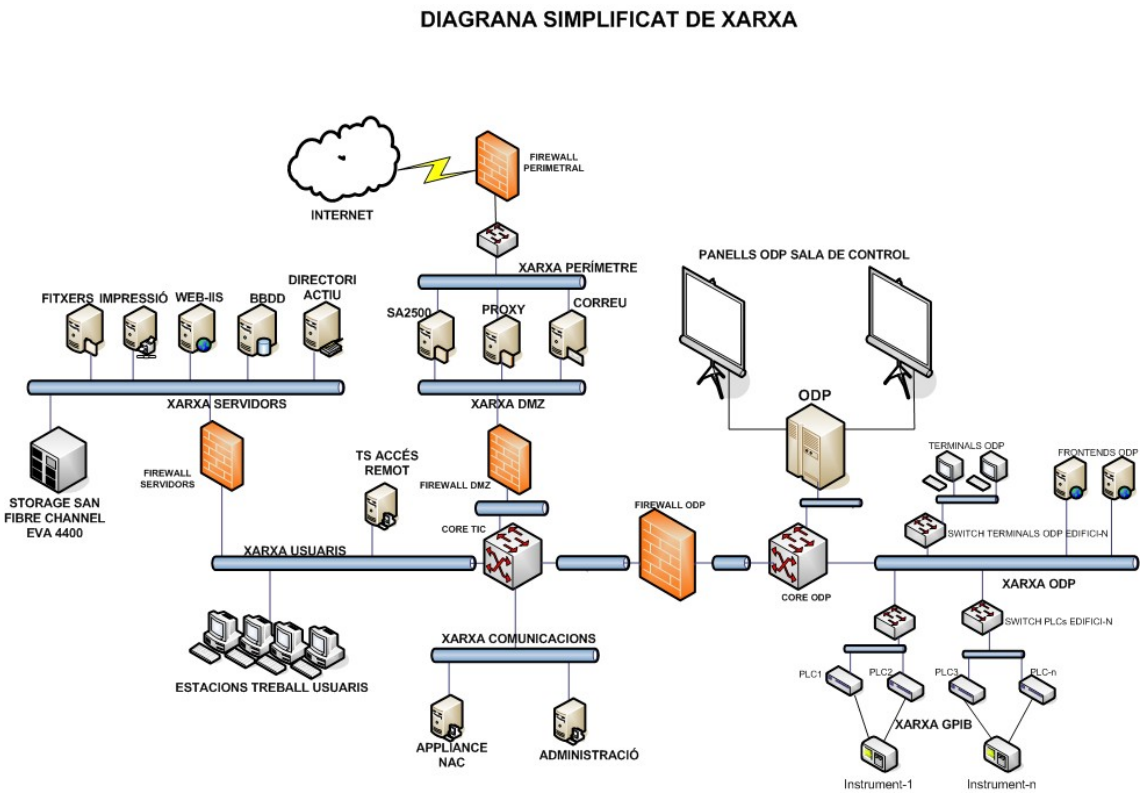
El CPD conta amb les mesures de seguretat següents:

- Control d'accessos personalitzat amb doble verificació (tarja+PIN)
- Dos línies d'alimentació independents que alimenten el SAI.
- Sistema d'alimentació ininterrompuda on-line (SAI) que permet apagar ordenadament els sistemes en cas de perduda d'alimentació.
- Sistema redundant d'aire condicionat.
- Sistema de detecció d'excés de temperatura.
- Sistema de detecció i extinció d'incendis automàtic.

- Detectors d'humitat i d'inundació
- Armari ignifug per guardar les copies de backup diàries.

En un edifici pròxim, dintre del perímetre de seguretat de la planta, TIC disposa d'un segon armari ignifug mes gran a on es conserven les copies de seguretat diàries (del dia anterior),setmanals, mensuals i anuals.

3.4.4-Diagrama simplificat de xarxa



4-Identificació d'actius, valoració del risc i amenaces

4.1-Introducció

Un cop que es disposa de la documentació que fa referència la **situació actual** de la empresa i **s'han definit els objectius del pla director de seguretat de la informació**, es necessari realitzar una **anàlisis del estat actual del risc** al que es troben sotmesos els actius crítics de la companyia.

És per això, que la primera etapa cap a la consecució del Pla Director consistirà en l'avaluació dels actius, considerant les dependències existents entre ells i realitzant una valoració.

Per poder dur a terme la valoració serà necessari completar cadascú dels següents apartats:

- Identificació i inventari d'actius
- Valoració dels actius
- Relació de la valoració amb les dimensions de la seguretat
- Anàlisi d'amenaces que afecten a cada actiu
- Càlcul de l'impacte potencial de cada amenaça sobre cada actiu
- Conclusions

Aquest es un proces iteratiu que s'haurà d'efectuar cada vegada que s'inclogui un nou actiu al inventari de la companyia, cada vegada que es realitzin canvis importants o periòdicament dintre del programa de millora continua de la empresa (PDCA).

4.2-Identificació d'actius de seguretat de la informació

Es denomina **actiu de seguretat de la informació** a la informació que te valor per l'organització i, per tant, s'ha de protegir en front de riscos i amenaces per assegurar el correcte funcionament del negoci.

Per fer mes comprensible el concepte, es pot assimilar la paraula **actiu**, dins d'aquest context, a un **element que conté o manipula (tracta) informació**.

En base a la definició anterior, un actiu d'informació pot ser: un fitxer, una base de dades, un contracte, documentació tècnica dels sistemes, aplicacions, software en general, maquinari (servidors, emmagatzemament en disc o dispositius extractables), serveis informàtics, comunicacions i persones que son las que, finalment, generen, alteren, transmeten o destrueixen la informació.

Tenir un inventari **d'actius crítics**, es el primer pas per poder dur a terme una avaluació de riscos.

Per tal de no tenir una explosió de dades desmesurada, els actius s'agruparan d'acord a la metodologia **MAGERIT** [2] en les següents categories:

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

4.3-Inventari d'actius

L'inventari d'actius haurà de recollir aquells elements que veritablement siguin significatius per l'organització, agrupant aquells que siguin similars, i tingui sentit la seva agrupació per tal de reduir l'extensió de l'inventari. Per exemple si existeixen 200 PCs d'usuari, amb les mateixes característiques, es podrien agrupar en un únic actiu denominat. **PC d'usuari**.

L'inventari d'actius ha de servir, també, per establir les relacions entre actius. Aquesta relació s'ha d'establir com un arbre de dependències entre actius. El concepte es que alguns actius depenen d'altres. Per exemple, una aplicació que resideixi en un servidor depèn d'aquest servidor per executar-se.

En una primera aproximació, els actius identificats es relacionaran a una taula a on s'establira, simplement, el seu grup de pertinença.

Agrupació/Tipus	Actiu
Instal·lacions	CPD GTEC CPD ODP Sala de Control Edifici del Reactor Edifici d'Administració Edifici de control d'accés a la instal·lació
Hardware GTEC Comunicacions	Firewall Perimetral Firewall DMZ GTEC Firewall ODP Firewall Servidors GTEC Equips de xarxa cablejada (switchs, routers,... etc.) Equips de xarxa sense fils (switchs, routers, punts d'accés, etc.) Appliance VPN SA2500
Hardware GTEC Servidors	Servidor BBDD GTEC Servidor Fitxers Servidor Impressió Servidor WEB-IIS GTEC Servidor Directori Actiu Servidor NAC Servidor administració comunicacions Servidor Correu Servidor Proxy Servidor TS Access Remot
Hardware GTEC PCs Escriptori	PC Escriptori
Hardware GTEC PCs Portàtils	PC Portàtils
Hardware GTEC Storage en Disc	EVA 4400 Storage en disc (SAN)
Hardware ODP Comunicacions	Equips de xarxa cablejada (switchs, routers,... etc.)
Hardware ODP Servidors	Servidor ODP Servidor Front-End ODP
Hardware ODP Panells	Panells ODP
Hardware ODP Terminals	Terminal ODP
Hardware ODP PLCs	PLC Siemens
Aplicació	GTEC ODP
Dades	Senyals ODP

Agrupació/Tipus	Actiu
	Catàleg Elements Tasques Manteniment Preventiu Sol·licituds de Treball Ordres de Treball Inventari Magatzem Proveïdors Comandes Informació de Personal Informació comptable Copies de seguretat dels sistemes
Xarxa GTEC	Xarxa Perimetral Xarxa DMZ GTEC Xarxa Comunicacions Xarxa Usuaris GTEC Xarxa Servidors GTEC
Xarxa ODP	Xarxa ODP Xarxa GPIB
Serveis GTEC	Accés usuaris interns, autenticació i autorització a sistemes Accés remot, autenticació i autorització a sistemes Serveis informàtics a usuaris (Espai de disc, correu electrònic, accés Internet, ...) Gestió Tècnica Gestió Econòmica Gestió de Personal
Serveis ODP	Monitorització i registre senyals de planta (ODP) Consulta externa senyals de planta (ODP)
Equipament auxiliar	Sistema contra incendis CPDs Sistema alimentació ininterrompuda CPDs Grup electrogen auxiliar Aire condicionat CPD
Personal	Direcció Personal TIC Reste Personal Plantilla Personal Extern

Taula 2: Relació d'actius amb grup *de pertinença*

4.4-Valoració d'actius

La valoració d'actius es una de les tasques mes complexes en el proces de avaluació de riscos. L'objectiu d'aquesta tasca es atorgar un valor a cada actiu, per tal de poder comparar aquest valor, amb el cost de les mesures de protecció que s'haurien d'aplicar a l'actiu. Així, si el cost de les mesures supera al valor de l'actiu, no tindria sentit la seva aplicació i s'haurien de cercar altres solucions.

Per valorar un actiu es poden fer servir dos aproximacions: quantitativa i qualitativa.

L'aproximació **quantitativa** tracta d'**assignar un valor econòmic real** a cada actiu. Aquesta valoració no es trivial i no sempre es possible ja que els actius no es valoren sempre per el seu cost sinó pel valor que representen per l'organització. Així, per exemple, seria molt complicat calcular el valor econòmic de la base de dades que conté les senyals del ordinador de processos definit en aquest Treball de Final de Màster **(TFM)**.

L'aproximació **qualitativa** estableix un **rang de valors [0,1,2,3,4,5]** o una **classificació en categories [Molt alt, Alt, Mig, Baix, Molt baix]** , per tal d'**establir el nivell d'importància que te l'actiu** per l'organització.

Per aquest TFM s'utilitzarà l'anàlisi que proposa **MAGERIT en e seu Llibre III (punt 2.1)** [3], completant-lo amb una estimació quantitativa, segons les següents categories:

Valor	Importància de l'actiu per l'organització	Justificació de la valoració
4	Molt alta	Es un actiu critic per l'organització, fonamental per la seguretat. El negoci no pot funcionar sense aquest actiu. Per exemple les dades de senyals de planta.
3	Alta	Es un actiu important per la seguretat, o del que depenen un o més actius crítics. El negoci pot veure reduïda, notablement, la seva activitat si l'actiu no està disponible. Per exemple el un dels PLC que registra senyals de planta.
2	Mitja	Es un actiu relacionat amb la seguretat o del que depenen actius importants. El negoci pot veure afectada, parcialment, la seva activitat si l'actiu no està disponible. Per exemple el servei de consulta externa de senyals de planta.
1	Baixa	Es un actiu que en cas de disponibilitat o mal funcionament representa un impacte baix per l'activitat del negoci. Per exemple una estació de consulta d'ODP o un PC d'escriptori
0	Menyspreable	Es un actiu que en cas de disponibilitat o mal funcionament representa un impacte pràcticament inexistent per l'activitat del negoci. Per exemple, un cable de xarxa o una impressora, ja que poden ser substituïts amb molta rapidesa. Aquest TFM no contempla aquest actius.

Taula 3: Criteris de valoració d'actius

Aquesta valoració tindrà en compte les relacions entre actius, de forma que els actius dependents d'altres hauran de propagar la seva categorització.

4.4.1-Relació de la valoració d'actius amb les dimensions de seguretat

Un cop identificats i valorats els actius, per cada un dels actius s'ha de mesurar la seva criticitat per cada una de les cinc dimensions de la seguretat de la informació (**ACIDT**): Autenticitat, Confidencialitat, Integritat, Disponibilitat, Traçabilitat.

Aquesta **valoració permetrà**, posteriorment, **avaluar l'impacte que tindrà la materialització d'una amenaça sobre la part de l'actiu exposat** (no cobert per les salvaguardes de cadascuna de les dimensions).

El valor que rebi l'actiu pot ser propi o acumulat. Així, els actius subordinats acumulen el valor dels actius que es recolzen en ells.

Per realitzar les ponderacions per cada actiu, s'ha de tenir en compte la importància o participació de l'actiu en la cadena de valor del servei, tractant d'evitar situacions del tipus “tot es molt important”, obligant, d'aquesta forma, als responsables de realitzar aquestes valoracions a discernir entre què es important i què no ho es tant.

Per tal de poder realitzar les valoracions de la criticitat de les dimensions de seguretat, s'utilitzarà una escala de deu valors segons els següents criteris:

Valor	Criteri	Justificació
10	Dany molt greu	Implica una interrupció total de les activitats del negoci
7-9	Dany greu	Implica una interrupció parcial de l'activitat del negoci
4-6	Dany important	Implica una reducció notable de l'activitat del negoci
1-3	Dany menor	Implica una reducció menor en l'activitat del negoci
0	Irrellevant	No te impacte en les activitats del negoci

Taula 4: Valoració de les dimensions de seguretat

4.5-Anàlisi d'amenaces

Dintre del context de la seguretat de la informació, una **amenaça** es la **probabilitat d'ocurrència d'un esdeveniment o acció que pot produir dany** (material o immaterial) sobre els actius d'informació.

El **dany** sobre un actiu pot afectar qualsevol de les seves dimensions de la seguretat (ACIDT), i serà **proporcional al grau d'exposició a la amenaça (vulnerabilitat)** que el provoca.

A nivell metodològic, s'analitzarà quines amenaces afecten als actius inventariats.

Posteriorment, s'analitzarà com es de vulnerable cada actiu a la materialització de l'amenaça, així com la freqüència estimada d'ocurrència d'aquesta.

En aquest TFM, s'utilitzaran les definides en **MAGERIT Llibre 2 “Catàleg**

d'elements" apartat 5 [4]. En aquest manual, les amenaces es troben classificades dins els següents grans blocs:

- [N] Desastres naturals
- [I] D'origen industrial
- [E] Errors i fallades no intencionades
- [A] Atacs intencionats

L'esmentat manual, a banda de definir amb detall la llista d'amenaces, **indica tant els tipus d'actius com les dimensions de la seguretat afectades per cadascuna**.

Per exemple, l'amenaça [A.5] suplantació de d'identitat de l'usuari,l presenta la següent taula d'afectacions.

[A.5] suplantació de d'identitat de l'usuari	
Tipus d'actius: • [S] serveis • [SW] aplicacions (software) • [COM] xarxes de comunicacions	**Dimensions:** 1. [C] confidencialitat 2. [A_S] autenticitat del servei 3. [A_D] autenticitat de les dades 4. [I] integritat
Descripció: • quan un atacant aconsegueix fer-se passar per un usuari autoritzat, gaudeix dels privilegis d'aquest per finalitats pròpies. • Aquesta amenaça pot ser perpetrada per personal intern, per personal alie a l'organització o per personal contractat temporalment.	

Taula 5: Descripció detallada d'una amenaça

Per aquest TFM i en base a l'experiència de l'alumne, es tindran en compte les següents dinou amenaces:

[N] – Desastres naturals

[N.1] Foc	
Tipus d'actius: • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar • [L] instal·lacions	**Dimensions:** 1. [D] disponibilitat 2. [T_S] traçabilitat dels serveis 3. [T_D] traçabilitat de les dades
Descripció: • incendis: possibilitat de que el foc malmeti recursos del sistema	

[N.2] Danys per aigua	
Tipus d'actius: • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar • [L] instal·lacions	**Dimensions:** 1. [D] disponibilitat 2. [T_S] traçabilitat dels serveis 3. [T_D] traçabilitat de les dades
Descripció: • inundacions: possibilitat de que l'aigua malmeti recursos del sistema	

[I] – D'origen industrial

[I.5] Avaria d'origen físic o lògic	
Tipus d'actius: • [SW] aplicacions, programari (software) • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar	**Dimensions:** 1. [D] disponibilitat 2. [T_S] traçabilitat dels serveis 3. [T_D] traçabilitat de les dades
Descripció: • fallades en els equips i/o fallades en els programes. Por ser deguda a un defecte d'origen o sobrevinguda durant el funcionament del sistema • en sistemes de propòsit específic, tal vegada es difícil saber si l'origen de la fallada es físic o lògic; però per les conseqüències que s'en deriven aquesta distinció sol ser irrellevant.	

[I.6] Tall de subministrament elèctric	
Tipus d'actius: • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar	**Dimensions:** 1. [D] disponibilitat 2. [T_S] traçabilitat dels serveis 3. [T_D] traçabilitat de les dades
Descripció: • cessament de l'alimentació elèctrica	

[I.7] Condicions anòmales de temperatura i/o humitat	
Tipus d'actius: • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar	**Dimensions:** 1. [D] disponibilitat 2. [T_S] traçabilitat dels serveis 3. [T_D] traçabilitat de les dades
Descripció: • diferències d'aclimatació a les instal·lacions excedint el marge de treball dels equips: excessiva calor, excessiu fred, excés d'humitat, ...	

[I.8] Fallada dels serveis de comunicacions	
Tipus d'actius: • [COM] xarxes de comunicacions	**Dimensions:** 1. [D] disponibilitat
Descripció: • cessament de la capacitat de transmetre dades d'un lloc a un altre. Típicament degut a la destrucció dels mitjans físics de transport o a la detenció dels centres de commutació, ja sigui per destrucció, detenció o simple incapacitat per atendre el tràfic present (saturació)	

[E] – Error i fallades no intencionades

[E.1] Errors dels usuaris	
Tipus d'actius: • [S] serveis • [D] dades / informació • [SW] aplicacions, programari (software)	**Dimensions:** 1. [I] integritat 2. [D] disponibilitat
Descripció: • equivocacions de les persones quan fan servir dades, serveis, etc.	

[E.2] Errors dels administradors	
Tipus d'actius: • [S] serveis • [D] dades / informació • [SW] aplicacions, programari (software) • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions	**Dimensions:** 1. [D] disponibilitat 2. [I] integritat 3. [C] confidencialitat 4. [A_S] autenticitat del servei 5. [A_D] autenticitat de les dades 6. [T_S] traçabilitat dels serveis 7. [T_D] traçabilitat de les dades
Descripció: • equivocacions de les persones amb responsabilitats de instal·lació i operació	

[E.20] Vulnerabilitat del programari (software)	
Tipus d'actius: • [SW] aplicacions, programari (software)	**Dimensions:** 1. [I] integritat 2. [D] disponibilitat 3. [C] confidencialitat
Descripció: • defectes el el codi que donen peu a una operació defectuosa sense intenció per part del usuari però amb conseqüències sobre la integritat de les dades o sobre la mateixa capacitat d'operar.	

[E.28] Indisponibilitat del personal	
Tipus d'actius: • [P] personal intern	**Dimensions:** 1. [D] disponibilitat
Descripció: • absència accidental del lloc de treball per: malaltia, alteració de l'ordre public, guerra, etc.	

[A] – Atacs intencionats

[A.8] Difusió de software maligne	
Tipus d'actius: • [SW] aplicacions, programari (software)	**Dimensions:** 1. [D] disponibilitat 2. [I] integritat 3. [C] confidencialitat 4. [A_S] autenticitat del servei 5. [A_D] autenticitat de les dades 6. [T_S] traçabilitat dels serveis 7. [T_D] traçabilitat de les dades
Descripció: • propagació intencionada de virus, spyware, cucs, troians, bombes lògiques, etc.	

[A.11] Access no autoritzat	
Tipus d'actius: • [S] serveis • [D] dades / informació • [SW] aplicacions, programari (software) • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar • [L] instal·lacions	**Dimensions:** 1. [C] confidencialitat 2. [I] integritat 3. [A_S] autenticitat del servei
Descripció: • l'atacant aconsegueix accedir als recursos del sistema sense disposar de la corresponent autorització, típicament aprofitant un error del sistema d'identificació i autorització .	

[A.15] Modificació de la informació	
Tipus d'actius: • [D] dades / informació	**Dimensions:** 1. [I] integritat
Descripció: • alteració intencionada de la informació amb ànim d'obtenir un benefici o de causar un prejudici.	

[A.16] Introducció de falsa informació	
Tipus d'actius: • [D] dades / informació	**Dimensions:** 1. [I] integritat
Descripció: • inserció intencionada d'informació falsa amb ànim d'obtenir un benefici o de causar un prejudici.	

[A.17] Corrupció de la informació	
Tipus d'actius: • [D] dades / informació	**Dimensions:** 1. [I] integritat
Descripció: • degradació intencionada de la informació amb ànim d'obtenir un benefici o de causar un prejudici.	

[A.18] Destrucció de la informació	
Tipus d'actius: • [D] dades / informació	**Dimensions:** 1. [D] disponibilitat
Descripció: • eliminació intencionada de la informació amb ànim d'obtenir un benefici o de causar un prejudici.	

[A.19] Divulgació de la informació	
Tipus d'actius: • [D] dades / informació	**Dimensions:** 1. [C] confidencialitat
Descripció: • revelació d'informació	

[A.25] Robatori	
Tipus d'actius: • [HW] equips informàtics (hardware) • [COM] xarxes de comunicacions • [SI] suports d'informació • [AUX] equipament auxiliar	**Dimensions:** 1. [D] disponibilitat 2. [C] confidencialitat
Descripció: • la sostracció d'equipament provoca, directament, la carència d'un mitja per prestar els serveis, es a dir, la indisponibilitat. • El robatori pot afectar a tot tipus d'equipament, sent el robatori d'equips i el robatori de suports d'informació els mes habituals. • El robatori el pot dur a terme personal intern, persones alienes a l'Organització o persones contractades de forma temporal, el que estableix diferents graus de facilitat per accedir a l'objecte sostret i diferents conseqüències. • En cas d'equips que emmagatzemen dades, també es pot patir una fuita d'informació.	

[A.28] Indisponibilitat del personal	
Tipus d'actius: • [P] personal intern	**Dimensions:** 1. [D] disponibilitat
Descripció: • absència deliberada del lloc de treball per: bagues, absentisme laboral, baixes no justificades, bloqueig d'accessos , etc.	

Com ja s'ha comentat, quan un actiu es víctima d'una amenaça, no es veu afectat en totes les seves dimensions ni en el mateix grau.

Un cop s'ha determinat que una amenaça pot perjudicar un actiu, s'ha d'estimar quan vulnerable es l'actiu en dos sentits:

degradació: quan perjudicat resultaria l'actiu

freqüència: cada quant es materialitza l'amenaça

La degradació mesura el perjudici causat per l'incident i s'acostuma a caracteritzar com una fracció del valor de l'actiu.

La freqüència posa en perspectiva aquella degradació, ja que una amenaça por ser de terribles conseqüències però de molt improbable materialització; mentre que altra amenaça, pot ser de molt baixes conseqüències però tant freqüent com per acumulat un prejudici considerable.

La freqüència es modela com una tassa anual d'ocurrència, sent els valor típics:

Valor normalitzat	Valor	Descripció	Justificació
4	100	Mont freqüent	A diari
3	10	Freqüent	mensualment
2	1	normal	Un cop l'any
1	1/10	Poc freqüent	Cada varis anys

Taula 6: Atribució de la freqüència

L'objectiu d'aquesta tasca es obtenir una taula resum a on per cada actiu s'identificaran les amenaces, la seva freqüència d'ocurrència i l'impacte sobre cada una de les dimensions de seguretat.

Com ja s'ha comentat, quan un actiu es víctima d'una amenaça, no es veu afectat en totes les seves dimensions ni en el mateix grau.

Un cop s'ha determinat que una amenaça pot perjudicar un actiu, s'ha d'estimar quan vulnerable es l'actiu en dos sentits:

degradació: quan perjudicat resultaria l'actiu

freqüència: cada quant es materialitza l'amenaça

La degradació mesura el perjudici causat per l'incident i s'acostuma a caracteritzar com una fracció del valor de l'actiu.

La freqüència posa en perspectiva aquella degradació, ja que una amenaça por ser de terribles conseqüències però de molt improbable materialització; mentre que altra amenaça, pot ser de molt baixes conseqüències però tant freqüent com per acumulat un prejudici considerable.

La freqüència es modela com una tassa anual d'ocurrència, sent els valor típics:

Valor normalitzat	Valor	Descripció	Justificació
4	100	Mont freqüent	A diari
3	10	Freqüent	mensualment
2	1	normal	Un cop l'any
1	1/10	Poc freqüent	Cada varis anys

Taula 7: Atribució de la freqüència

L'objectiu d'aquesta tasca es obtenir una taula resum a on per cada actiu s'identificaran les amenaces, la seva freqüència d'ocurrència i l'impacte sobre cada una de les dimensions de seguretat.

		Degradació				
Actiu		**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Actiu analitzat		**50%**	**60%**	**100%**	**10%**	**90%**
Amenaces sobre l'actiu	**Freqüència**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[E.1] Errors dels usuaris	1			10%	10%	
[E.16] Introducció false d'informació	100			50%		
[A.4] Manipulació de la configuració	1/10	50%	60%	70%	5%	90%
[A.16] Introducció false d'informació	10			100%		

Taula 8: Actius, amenaces i impacte en dimensions de seguretat

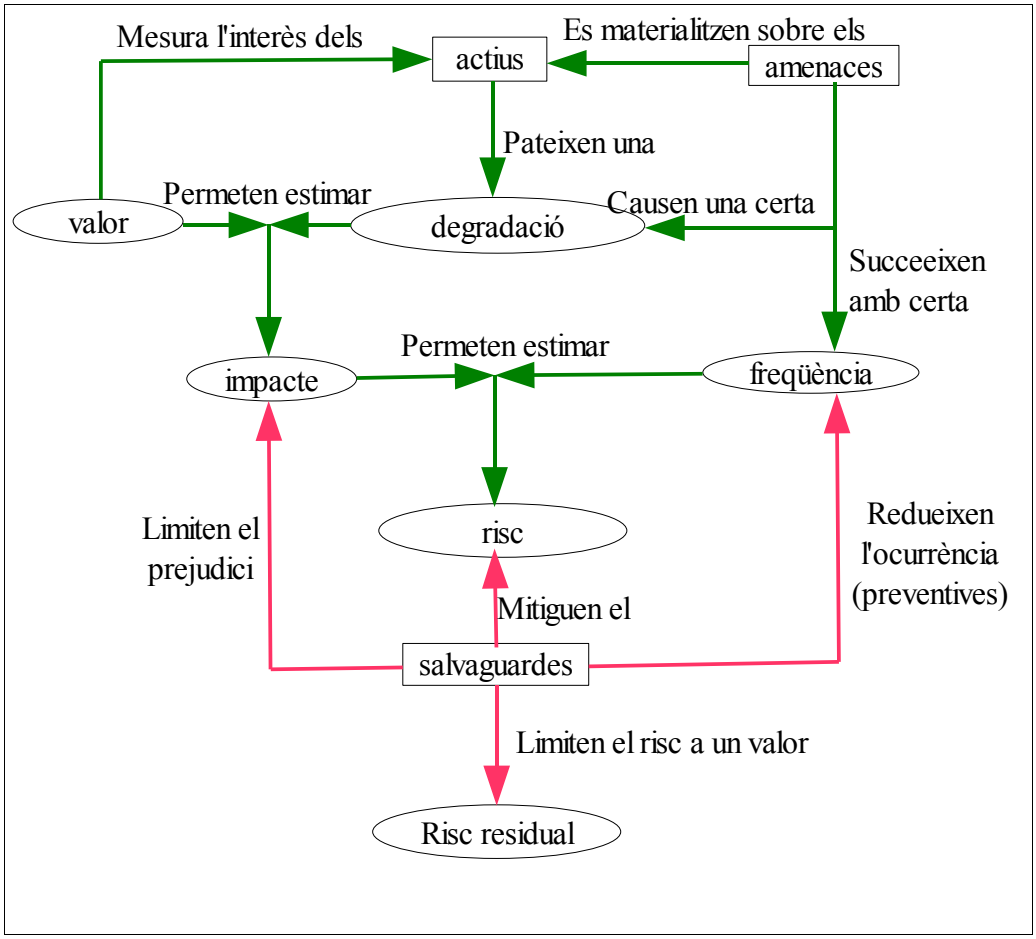
Com es pot veure, l'actiu, en cada una de les dimensions de seguretat, presenta el **màxim impacte** de cada una amenaces avaluades.

4.6-Determinació de l'impacte

Amb la taula anterior i amb el coneixement previ del valor dels actius i de les relacions que existeixen entre ells, es determinarà risc que pot suposar per l'organització la materialització de les amenaces.

Aquesta dada permetrà prioritzar el pla d'acció, i, alhora, avaluar com es modificarà aquest quan s'hagin aplicat les contramesures.

Per donar una idea de conjunt d'on s'utilitzarà cada una de les dades obtingudes, cal revisar el següent esquema inclòs al **Libro_I_Metodo de la metodologia MAGERIT V2 a la pàgina 132** [5]:



Dibuix 1: Proces d'estimació del risc

4.7-Anàlisi de riscos NUCSSION

Per tal de no fer molt gran l'explosió combinatòria d'aquesta anàlisi, la avaluació de riscos es centrarà en els **serveis** de **Accés usuaris interns, autenticació i autorització a sistemes**, **Gestió Tècnica**, **Consulta senyals de planta ODP** i **Monitorització i registre senyals de planta** que depenen de múltiples actius i **representen la informació i serveis mes crític**s de l'organització.

Seguint la metodologia MAGERIT d'anàlisi de riscos, segons el mètode descrit a la pàgina 37 del **Libro_I_Método** [5], es desenvoluparà el proces **P2: Anàlisi de riscos.**

Aquest proces es divideix en quatre activitats i cada una d'elles en tasques que cal completar per aconseguir l'objectiu final.

P2: Anàlisi de riscos

- Activitat A2.1: Caracterització dels actius
  - Tasca T2.1.1: Identificació dels actius
  - Tasca T2.1.2: Dependència entre actius
  - Tasca T2.1.3: Valoració dels actius
- Activitat A2.2: Caracterització de les amenaces
  - Tasca T2.2.1: Identificació de les amenaces
  - Tasca T2.2.2: Valoració de les amenaces
- Activitat A2.3: Caracterització de les salvaguardes
  - Tasca T2.3.1: Identificació de les salvaguardes existents
  - Tasca T2.3.2: Valoració de les salvaguardes existents
- Activitat A2.4: Estimació de l'estat del risc
  - Tasca T2.4.1: Estimació de l'impacte
  - Tasca T2.4.2: Estimació del risc
  - Tasca T2.4.3: Interpretació dels resultats

4.7.1-Activitat A2.1: Caracterització dels actius

4.7.1.1-Tasca T2.1.1: Identificació dels actius

El resultat d'aquesta tasca ha quedat plasmat en la Taula 1: Relació d'actius amb grup de pertinença. En aquesta taula es relacionen els actius de l'organització, agrupant aquells que son del mateix tipus (p.ex. Firewall, PCs Usuari, etc.) i categoritzant-los segons al tipus al que pertanyen (Instal·lacions, Hardware, etc.).

4.7.1.2-Tasca T2.1.2: Dependència entre actius

Segons la llista d'actius identificats en el pas anterior i pels actius seleccionats per realitzar aquesta avaluació de riscos, es mostra la següent taula de dependències:

ACTIU		
Accés usuaris interns, autenticació i autorització a sistemes	**DEPENDÈNCIA**	**UBICACIÓ**
	Xarxa Usuaris	Instal·lacions NUCSSION
	Xarxa Servidors	CPD GTEC
	Firewall Servidors	CPD GTEC
	PC Usuari	Instal·lacions NUCSSION
	Servidor Active Directory	CPD GTEC
	CPD GTEC	Instal·lacions NUCSSION
	Personal TIC	-
	Resta Personal	-

ACTIU		
Gestió Tècnica	**DEPENDÈNCIA**	**UBICACIÓ**
	Xarxa Usuaris	Instal·lacions NUCSSION
	Xarxa Servidors	CPD GTEC
	Firewall Servidors	CPD GTEC
	PC Usuari	Instal·lacions NUCSSION
	Servidor Web-IIS GTEC	CPD GTEC
	Servidor BBDD GTEC	CPD GTEC
	Catàleg Elements	Servidor BBDD GTEC
	Tasques MP	Servidor BBDD GTEC

	Sol·licituds de treball	Servidor BBDD GTEC
	Ordres de treball	Servidor BBDD GTEC
	STORAGE SAN	CPD GTEC
	CPD GTEC	Instal·lacions NUCSSION
	Edifici Administració	Instal·lacions NUCSSION
	Personal TIC	-
	Resta Personal	-

ACTIU		
Consulta externa senyals de planta (ODP)	**DEPENDÈNCIA**	**UBICACIÓ**
	Xarxa ODP	CPD ODP
	Firewall ODP	CPD GTEC
	Xarxa Usuaris	Instal·lacions NUCSSION
	PC Usuari	Instal·lacions NUCSSION
	Servidor ODP	CPD ODP
	FrontEnds ODP	CPD ODP
	Servidor Web-IIS GTEC	CPD GTEC
	Senyals ODP	Servidor ODP
	CPD ODP	Instal·lacions NUCSSION
	CPD GTEC	Instal·lacions NUCSSION
	Edifici Administració	Instal·lacions NUCSSION
	Personal TIC	-
	Resta Personal	-

ACTIU		
Monitorització i registre senyals de planta (ODP)	**DEPENDÈNCIA**	**UBICACIÓ**
	Xarxa ODP	CPD ODP
	Servidor ODP	CPD ODP
	Panells ODP Sala Control	Sala de Control
	PLC Siemens	Edifici Reactor
	Xarxa GPIB	Edifici Reactor
	Instrument	Edifici Reactor
	Senyals ODP	Servidor ODP
	CPD ODP	Instal·lacions NUCSSION
	Sala de control	Instal·lacions NUCSSION
	Edifici Reactor	Instal·lacions NUCSSION
	Personal TIC	-
	Resta Personal	-

Taula 9: Dependències entre actius

4.7.1.3-Tasca T2.1.3: Valoració dels actius

Un cop identificats els actius i les seves dependències s'ha d'assignar una valoració a cada actiu principal, en cada una de les seves dimensions. Per poder unificar criteris de valoració s'utilitzarà, un qüestionari i la guia de valoració definida per les taules que publica **MAGERIT V2 al seu Llibre_II_Catàleg_d'Elements, apartat 4.1 Escala estàndard** [4]. Amb aquests documents, es realitzaran entrevistes amb cada usuari responsable de l'actiu analitzat. El qüestionari i les taules de valoració s'adjuntaran, com annexes a aquest TFM.

El qüestionari, recollirà una serie de respostes de l'usuari responsable que permetran mesurar l'impacte en cada una de les dimensions de seguretat per l'actiu avaluat, assignant un valor d'una de les taules emprades. Un exemple d'aquest qüestionari s'adjunta a l'annexe 1 d'aquest document.

Un cop recollida la informació amb els qüestionaris, amb un full de càlcul, s'ha construït una taula a un es relacionen els actius a analitzar, junt amb les

seves dependències (actius dependents). Aquest full de càlcul s'adjuntarà com documentació addicional a aquest TFM.

Per cada actiu **principal**, es detallen les valoracions a cada una de les seves dimensions.

Posteriorment, cada actiu **depenent** es relaciona amb els actius principals als que afecta i es calculen els valors per cada una de les dimensions com el màxim valor en cada una de les dimensions dels actius principals.

Actiu			**A**	**C**	**I**	**D**	**T**
Actiu P1			**2**	**4**	**5**	**4**	**1**
Actiu P2			**1**	**7**	**3**	**6**	**2**
	AP1	**AP2**					
Actiu D1	1	1	**2**	**7**	**5**	**6**	**2**
Actiu D2		1	**1**	**7**	**3**	**6**	**2**
Actiu D3	1		**2**	**4**	**5**	**4**	**1**

Taula 10: Valoració d'actius

Com es pot veure a la taula anterior, els actius principals P1 i P2 presenten els seus valors assignats després de l'entrevista amb els seus propietaris.

Els actius dependents (o subordinats) D1, D2 i D3 expressen la seva relació amb P1 i P2 mitjançant el valor **1** present a les columnes **AP1 i AP2**.

La formula per calcular el valor de les dimensions de seguretat de cada actiu subordinat, es:

suposem calcular la dimensió Disponibilitat (D) per l'actiu depenent D1

MAX(Actiu D1.AP1*Actiu P1.D; Actiu D1.AP2*Actiu P1.D) =

MAX(1*4;1*6) = **6**

El mateix cas però ara per l'actiu depenent D3

MAX(Actiu D3.AP1*Actiu P1.D; Actiu D3.AP2*Actiu P1.D) =

MAX(1*4;0*6) = **4**

4.7.2-Activitat A2.2: Caracterització de les amenaces

4.7.2.1-Tasca T2.2.1: Identificació de les amenaces

En aquest apartat, s'han identificat una serie d'amenaces que poden afectar els actius sobre els que es farà aquest estudi i s'ha obtingut el grau de degradació que representaria que la amenaça es materialitzes, així com la seva freqüència d'ocurrència.

S'ha pres altre cop la llista d'amenaces definida a **MAGETIT V2 Llibre 2 "Catàleg d'elements" apartat 5** [4], com s'ha comentat anteriorment.

4.7.2.2-Tasca T2.2.2: Valoració de les amenaces

Seguint amb el full de càlcul, per cada actiu (principal i depenent) s'ha fer un anàlisi de cada una de les amenaces en les dimensions que assenyala MAGERIT per cada una d'elles.

Posteriorment, s'ha pres el màxim valor de degradació per cada dimensió i el valor de la freqüència màxima normalitzada(valors entre 1 i 4 segons taula: 5).

Els valors que representen la degradació de cada una de les dimensions està expressat en percentatge.

Els valors que representen la freqüència d'ocurrència estan expressats com taxa anual.

Actiu		A	C	I	D	T
PLC SIEMENS	2	20	100	100	100	20
AMENACES	Freqüència					
[N.1] Foc	1				100	
[N.2] Danys per aigua	1				100	
[I.5] Avaria d'origen físic o lògic	1				100	
[I.6] Tall de subministrament elèctric	1				100	
[I.7] Condicions anòmales de temperatura i/o humitat	1				100	
[I.8] Fallada dels serveis de comunicacions	1				100	
[E.1] Errors dels usuaris						
[E.2] Errors dels administradors	2	20	20	20	50	20
[E.20] Vulnerabilitat del programari (software)	1		100	100	100	
[E.28] Indisponibilitat del personal						
[A.8] Difusió de software maligne						
[A.11] Accés no autoritzat	1			100		
[A.15] Modificació d'informació	1			100		
[A.16] Introducció de falsa informació	1			100		
[A.17] Corrupció d'informació	1			100		
[A.18] Destrucció d'informació	1				100	
[A.19] Divulgació d'informació						
[A.25] Robatori						
[A.28] Indisponibilitat del personal						

Taula 11: Assignació de percentatge de degradació i freqüència d'ocurrència

4.7.3-Activitat A2.3: Caracterització de les salvaguardes

4.7.3.1-Tasca T2.3.1: Identificació de les salvaguardes existents

En els passos anteriors **s'ha tingut en compte les salvaguardes desplegades en cada actiu**, tal i com estan descrites en el document de FASE2 d'aquest TFM.

Les salvaguardes afecten el càlcul del risc de dos maneres:

- Reduint la freqüència d'ocurrència de les amenaces.
  - Aquestes salvaguardes s'anomenen preventives. Una salvaguarda preventiva ideal mitiga completament l'amenaça.
- Limitant el dany causat
  - Existeixen salvaguardes que directament limiten la possible degradació, mentre que altres, permeten detectar, immediatament, un atac per tal de frenar que la degradació avanci.

4.7.3.2-Tasca T2.3.2: Valoració de les salvaguardes existents

Aquest TFM NO REALITZA VALORACIÓ DE SALVAGUARDES EXISTENTS i es limita a valorar els actius amb les salvaguardes que tenen aplicades.

A mode de recordatori, se enuncien algunes de les salvaguardes aplicades:

- La xarxa de la empresa es ta segmentada en dos grans blocs, la part de gestió i la part de proces. La part de gestió, es troba també segmentada segons criteris de ubicació d'equips i serveis.
- Tot el trànsit entre els diferents segments de xarxa està controlat per firewalls que filtren els accessos permetent, únicament, el tràfic autoritzat.
- Tots els servidors conten amb antivírics instal·lat i actualitzat diàriament.
- Tots els servidors crítics o importants compten amb alta disponibilitat o balanceig de carrega.
- Les estacions de treball es troben auditades, permanentment, per un sistema NAC i els usuaris no disposen de privilegis d'administració.
- Tota la gestió de usuaris/contrasenyes està basada en active directori.
- Sols els administradors tenen permisos d'instal·lador i operador per manegar contes d'usuari i permisos d'accés.
- No existeix un usuari únic i genèric administrador del sistema. Cada usuari disposa de les seves credencials i s'auditen les seves accions al sistema.
- Tots els edificis, incloent els CPDs disposen de sistemes redundants d'aire condicionat, sistemes d'alimentació ininterrompuda i generadors dièsel auxiliars per previndré problemes de tall de subministrament elèctric.
- Es fan copies de seguretat diàries, incrementals i diferencials i les cintes es guarden dintre d'armaris ignífugs. Diàriament les copies del dia anterior es traslladen a un bunker especial.
- Existeixen fortes mesures de seguretat física basades en barreres, vigilants de seguretat armats i targetes d'accés personal que garanteixen que sols poden accedir al emplaçament les persones degudament autoritzades.
- L'accés remot des-de l'exterior es fa amb una doble validació: usuari+contrasenya+tocken RSA

4.7.4-Activitat A2.4: Estimació de l'estat del risc

4.7.4.1-Tasca T2.4.1: Estimació de l'impacte

S'anomena **impacte** a la mesura del dany sobre l'actiu, derivat de la materialització d'una amenaça. Coneixent el valor dels actius en cada una de les seves dimensions i la degradació que provoquen les amenaces, es directa derivar l'impacte que aquestes amenaces tindrien sobre el sistema.

La formula per calcular l'impacte es: **I = round(V * d**) on **I** serà el resultat del impacte calculat per una dimensió d'un actiu, **V** serà el valor de l'actiu per una dimensió concreta y **d** serà la degradació calculada per aquella dimensió en funció de les amenaces

La funció **round**, arrodoneix el nombre al següent enter si la part decimal e >= 5, es a dir 5.6 serà arrodonit a 6. D'altra banda, si la part decimal es <5, la funció **round** arrodoneix depreciant la part decimal i quedat-se amb la part sencera, es a dir 5.4, quedaria com 5.

Es important destacar que l'impacte s'ha de calcular per cada una de les dimensions de seguretat de cada actiu.

Novament el full de càlcul permet realitzar el càlcul d'aquesta variable (impacte), en base als càlculs realitzats anteriorment.

La taula a emprar disposa de la relació de tots els actiu que s'han valorat amb el màxim valor per cada dimensió de seguretat. En una columna adjacent, es fa el càlcul de l'impacte en base al valor de cada dimensió de cada actiu i la degradació que cada actiu presenta en cada una de les seves dimensions en base a la taula de valoració d'amenaces.

	VALOR MAX. DIMENSIÓ					VALOR DE L'IMPACTE				
	A	C	I	D	T	A	C	I	D	T
ACTIU										
Accés usuaris interns, autenticació i autorització a sistemes	7	7	7	8	7	1	6	7	2	1
Servidor Active Directory	7	7	7	8	7	1	7	7	8	1
CPD ODP	2	2	8	8	2	0	2	8	8	0
Firewall ODP	2	2	6	4	2	0	2	5	4	2

Taula 12: Càlcul de l'impacte

Com exemple, per primer actiu, el valors de degradació, expressats en tant per cent, assignats per cada una de les dimensions han estat els següents:

	A	C	I	D	T
ACTIU					
Accés usuaris interns, autenticació i autorització a sistemes	**20**	**80**	**100**	**20**	**20**

Es immediat comprovar el resultat de la taula anterior:

A: round(7*20%) = 1

C: round(7*80%) = 6

I: round(7*100%) = 7

D: round(8*20%) = 2

T: round(7*20%) = 1

4.7.4.2-Tasca T2.4.2: Estimació del risc

Es l'ultim pas en el proces d'avaluació de riscos. Amb tota la informació anterior disponible, per obtenir el risc associat a cada actiu sols queda fer el càlcul per cada actiu i dimensió, prenen el valor de l'impacte i la freqüència d'ocurrència.

Per tal d'obtenir uns valors normalitzats, s'utilitzarà una funció que tornara un enter entre 1 i 7. Aquest valor serà funció de l'impacta i de la freqüència màxima acumulada d'ocurrència d'una amenaça per cada actiu.

Per realitzar els càlculs es prendrà com origen la taula emprada pel càlcul de l'impacte (Taula: 10), estenent-la com es mostra a continuació:

RISC	VALOR MAX. DIMENSIÓ					VALOR DE L'IMPACTE					VALOR RISC					RISC
	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	MÀXIM
ACTIU																
Accés usuaris interns, autenticació i autorització a sistemes	7	7	7	8	7	1	6	7	2	1	2	5	5	3	2	5
Servidor Active Directory	7	7	7	8	7	1	7	7	8	1	2	5	5	5	2	5
CPD ODP	2	2	8	8	2	0	2	8	8	0	1	2	5	5	1	5
Firewall ODP	2	2	6	4	2	0	2	5	4	2	1	2	4	3	2	4

Taula 13: Estimació del risc

La funció que obté la estimació del risc es la següent:

Al valor de l'impacte de cada dimensió se li suma el valor màxim de la freqüència d'ocurrència(segons taula d'amenaces) mes una constant, en aquest cas 2. El resultat obtingut es divideix per 2. amb aquesta funció el valor mínim obtingut es 2 (1+1+2)/2 i el màxim 8 (10+4+2)/2.

D'aquesta manera s'obtenen resultats normalitzats i uniformes per poder realitzar, posteriorment, les accions pertinents per tal de reduir el risc.

EL DESPLEGAMENT TOTAL DE LES TAULES ES POR VEURE EN L'ARXIU QUE S'ADJUNTA AMB AQUESTA MEMORIA:

RubioRodriguezEnrique_TFM_riscos.ods

5-Nivell de compliment actual

5.1-Introducció i metodologia

Un cop que es coneixen els actius de l'empresa i s'han avaluat les amenaces es el moment d'avaluar fins quin punt l'empresa compleix amb les bones pràctiques en matèria de seguretat. El marc de control de la seguretat es desenvoluparà en base a la **norma ISO/IEC-27002:2005** [6]. Conjuntament amb l'anàlisi de riscos, permetrà plantejar un conjunt de projectes per a la millora de la seguretat de l'organització. Aquest conjunt de projectes seran la base del pla d'acció del pla director.

5.2-Avaluació de la maduresa

L'objectiu d'aquesta fase del projecte és avaluar la maduresa de la seguretat pel que fa als diferents dominis de control i els 133 controls plantejats per la ISO / IEC 27002:2005. Abans d'abordar aquesta avaluació s'ha d'aprofundir al màxim en el coneixement de l'organització.

De forma resumida, els dominis que s'han d'analitzar són:

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

L'estudi ha de fer una revisió dels 133 controls plantejats per la norma per complir amb els diferents objectius de control - el nombre dels quals pot ser donada per a cada un dels dominis-.

Aquesta estimació es durà a terme segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	**L0**	Inexistent	Manca completa de qualsevol procés recognoscible. No s'ha reconegut si més no que hi ha un problema a resoldre.
10%	**L1**	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la majoria de les vegades en l'esforç personal. Els procediments són inexistents o localitzats en àrees concretes. No hi ha plantilles definides a nivell corporatiu.
50%	**L2**	Reproduïble, però intuïtiu	Els processos similars es porten en forma similar per diferents persones amb la mateixa tasca. Es normalitzen les bones pràctiques sobre la base de l'experiència i al mètode. No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	**L3**	Proces Definit	L'organització sencera participa en el procés. Els processos estan implantats, documentats i comunicats mitjançant entrenament.
95%	**L4**	Gestionat i mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, es tenen eines per millorar la qualitat i l'eficiència.
100%	**L5**	Optimitzat	Els processos estan sota constant millora. En base a criteris quantitatius es determinen les desviacions més comuns i s'optimitzen els processos.

Taula 14: Efectivitat dels controls

Per tal de poder dur a terme aquesta tasca, per cada un del controls de la norma ISO/IEC-27002:2005, s'haurà de respondre una pregunta d'auditora. La resposta determinarà el grau de compliment del control, del que, posteriorment, se'n podrà derivar el nivell de maduresa.

Com eina de suport per respondre les preguntes i poder obtenir les gràfiques de mode automàtic, per aquest TFM s'han construït una serie de fulls de càlcul, agrupats en un llibre.

Quant a la resposta d'auditoria que s'haurà de respondre per cada un dels controls, s'ha triat el següent model:

La resposta tindrà quatre possibles valors:

- SI
- NO
- PARCIALMENT
- NO APLICA

Cada domini de seguretat, dels 11 que defineix la norma, consta de un número determinats de controls agrupats en objectius. Per aquest TFM sols s'ha tingut en compta els controls.

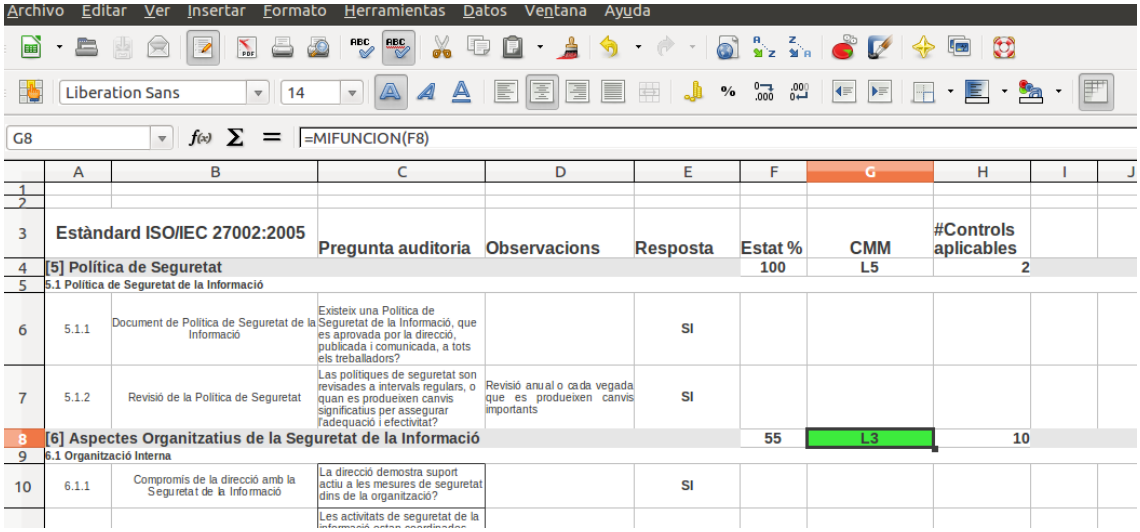
El grau de compliment del 100 % d'un domini de seguretat implicarà que tots els seus controls estiguin implantats, es a dir, la implantació de cada control aporta un cert percentatge de compliment al control. Per exemple pel domini de seguretat ***[8] Seguretat relacionada amb els recursos humans***, la norma defineix nou (9) controls. Seguint el raonament anterior, el compliment TOTAL de cada un d'aquest controls aportaria un 100/9% del compliment, es a dir un 11,12%.

Amb el model proposat, cada resposta **SI** acumularà un percentatge equivalen a **100/numero de controls**. Una resposta **NO** sumarà **cero (0)** al percentatge de compliment. Una resposta **PARCIALMENT**, aportarà **la meitat d'una resposta SI.** Una resposta **NO APLICA,** no tindrà en compta aquest

control pel calcul del compliment. Es a dir, en el cas de l'anterior domini que en tenia 9 controls, si un d'ells es marqués com NO APLICA, els càlculs es farien, sobre 8 controls en contes de sobre els 9 controls originals del domini.

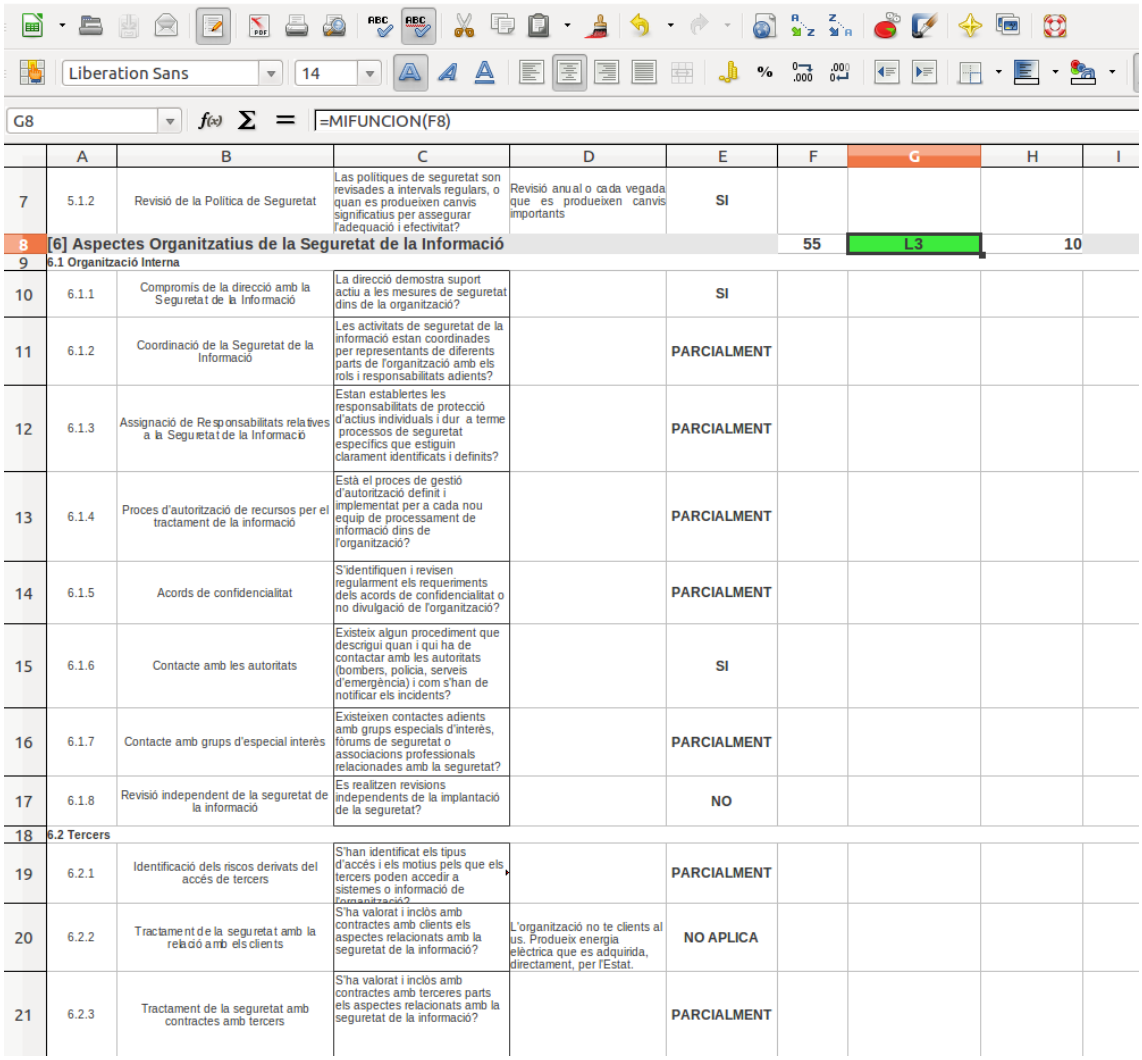
No s'ha disposat del temps per programar al full de càlcul aquesta ultima reducció del numero de controls a aplicar, pel que s'ha hagut d'indicar manualment, es a dir, descomptant el numero de controls que NO APLIQUEN per cada domin de seguretat.

Com exemple, en la pàgina següent es presenta una captura del full de càlcul que acompanya a aquesta part del TFM **RubioRodriguezEnrique_TFM_Controls.ods**



	A	B	C	D	E	F	G	H	I	J
3	Estàndard ISO/IEC 27002:2005		Pregunta auditoria	Observacions	Resposta	Estat %	CMM	#Controls aplicables		
4	[5] Política de Seguretat					100	L5	2		
5	5.1 Política de Seguretat de la Informació									
6	5.1.1	Document de Política de Seguretat de la Informació	Existeix una Política de Seguretat de la Informació, que es aprovada por la direcció, publicada i comunicada, a tots els treballadors?		SI					
7	5.1.2	Revisió de la Política de Seguretat	Las polítiques de seguretat son revisades a intervals regulars, o quan es produeixen canvis significatius per assegurar l'adequació i efectivitat?	Revisió anual o cada vegada que es produeixen canvis importants	SI					
8	[6] Aspectes Organitzatius de la Seguretat de la Informació					55	L3	10		
9	6.1 Organització Interna									
10	6.1.1	Compromís de la direcció amb la Seguretat de la Informació	La direcció demostra suport actiu a les mesures de seguretat dins de la organització?		SI					

Il·lustració 4: Full de càlcul amb les capçaleres



	A	B	C	D	E	F	G	H	I
7	5.1.2	Revisió de la Política de Seguretat	Las polítiques de seguretat son revisades a intervals regulars, o quan es produeixen canvis significatius per assegurar l'adequació i efectivitat?	Revisió anual o cada vegada que es produeixen canvis importants	SI				
8	[6] Aspectes Organitzatius de la Seguretat de la Informació					55	L3	10	
9	6.1 Organització Interna								
10	6.1.1	Compromís de la direcció amb la Seguretat de la Informació	La direcció demostra suport actiu a les mesures de seguretat dins de la organització?		SI				
11	6.1.2	Coordinació de la Seguretat de la Informació	Les activitats de seguretat de la informació estan coordinades per representants de diferents parts de l'organització amb els rols i responsabilitats adients?		PARCIALMENT				
12	6.1.3	Assignació de Responsabilitats relatives a la Seguretat de la Informació	Estan establertes les responsabilitats de protecció d'actius individuals i dur a terme processos de seguretat específics que estiguin clarament identificats i definits?		PARCIALMENT				
13	6.1.4	Proces d'autorització de recursos per el tractament de la informació	Està el proces de gestió d'autorització definit i implementat per a cada nou equip de processament de informació dins de l'organització?		PARCIALMENT				
14	6.1.5	Acords de confidencialitat	S'identifiquen i revisen regularment els requeriments dels acords de confidencialitat o no divulgació de l'organització?		PARCIALMENT				
15	6.1.6	Contacte amb les autoritats	Existeix algun procediment que descrigui quan i qui ha de contactar amb les autoritats (bombers, policia, serveis d'emergència) i com s'han de notificar els incidents?		SI				
16	6.1.7	Contacte amb grups d'especial interès	Existeixen contactes adients amb grups especials d'interès, fòrums de seguretat o associacions professionals relacionades amb la seguretat?		PARCIALMENT				
17	6.1.8	Revisió independent de la seguretat de la informació	Es realitzen revisions independents de la implantació de la seguretat?		NO				
18	6.2 Tercers								
19	6.2.1	Identificació dels riscos derivats del accés de tercers	S'han identificat els tipus d'accés i els motius pels que els tercers poden accedir a sistemes o informació de l'organització?		PARCIALMENT				
20	6.2.2	Tractament de la seguretat amb la relació amb els clients	S'ha valorat i inclòs amb contractes amb clients els aspectes relacionats amb la seguretat de la informació?	L'organització no te clients al us. Produeix energia elèctrica que es adquirida, directament, per l'Estat.	NO APLICA				
21	6.2.3	Tractament de la seguretat amb contractes amb tercers	S'ha valorat i inclòs amb contractes amb terceres parts els aspectes relacionats amb la seguretat de la informació?		PARCIALMENT				

Il·lustració 5: Exemple complert d'un domini de seguretat

Com es pot veure a la il·lustració, el valor total del percentatge de compliment es el 55%. El número de controls a aplicar a aquest domini, segons la norma es de 11, però com es pot veure a la mateixa línia del percentatge i del grau de CMMI, el número de controls aplicables, en aquest cas, es de 10, ja que un dels controls NO APLICA (amb la corresponent justificació).

Quant a la relació del compliment percentual amb la proposta de CMM del equip docent, ha quedat de la següent forma:

Si el percentatge de compliment es 0% llavors Nivell CMM = L0

Si el percentatge de compliment està entre 1% i 10% llavors Nivell CMM = L1

Si el percentatge de compliment està entre 11% i 50% llavors Nivell CMM = L2

Si el percentatge de compliment està entre 51% i 90% llavors Nivell CMM = L3

Si el percentatge de compliment està entre 91% i 95% llavors Nivell CMM = L4

Si el percentatge de compliment es mes gran el 95% llavors Nivell CMM = L5

Com exemple es pot veure la macro implementada en **libre office** per calcular el nivell de CMM:

```
REM  *****  BASIC  *****
Option Explicit

Function MiFuncion(valor as integer) As String

    dim retval as string
    retval = "L0"

    if valor >1  and valor <=10 then retval = "L1"
    if valor >10 and valor <=50 then retval = "L2"
    if valor >50 and valor <=90 then retval = "L3"
    if valor >90 and valor <=95 then retval = "L4"
    if valor >95 then retval = "L5"

      MiFuncion = retval

End Function
```

Aquesta distribució, fa que la majoria dels dominis es trobin en un nivell de compliment CMM de L2 i L3. Crec que es podria ajustar una mica per tal de obtenir mes L2 i, posteriorment, realitzar un proces d'implantació de millores per assolir el nivell L3 en tots els controls.

5.3-Presentació de resultats

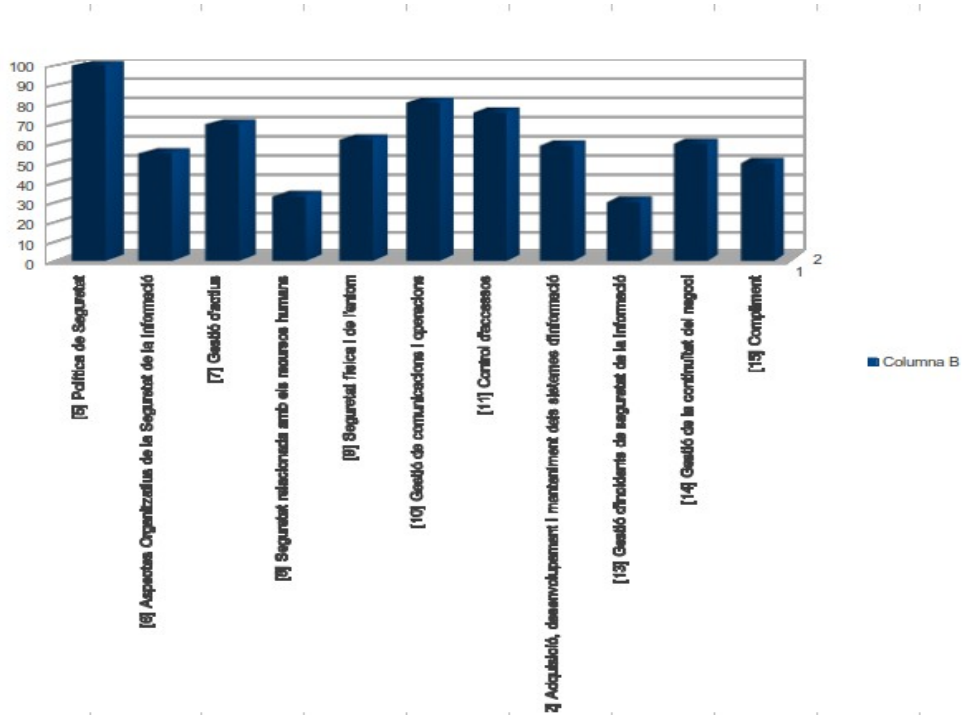
Aquest apartat ha estat una mica complex ja que mai no havia treballat amb gràfics d'**excel** o **libre office**.

En primer gràfic que es presenta es el resultat numèric de la situació:

%Compliment	CMM	controls aplicables	controls totals
100	L5	2	2
55	L3	10	11
70	L3	5	5
33	L2	9	9
62	L3	13	13
81	L3	29	32
76	L3	23	25
59	L3	16	16
30	L2	5	5
60	L3	5	5
50	L2	10	10
%Compliment	CMM	controls aplicables	controls totals
61	L3	127	133

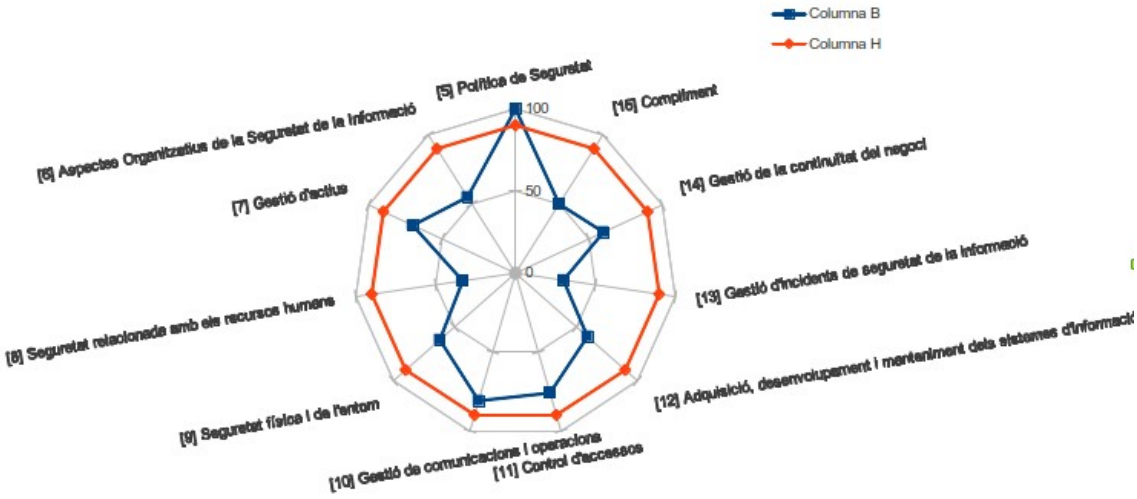
Il·lustració 6: Resultat numèric de la situació

El següent, correspon a un gràfic de barres a on es presenta la informació en percentatges de compliment per cada domini de seguretat:



Il·lustració 7: Diagrama de barres en percentatge

A continuació es presenta el diagrama de radar a on es pot veure en vermell l'objectiu al que l'organització aspira (L3) i en blau la situació actual (també percentual).



Il·lustració 8: Diagrama de radar o de xarxa amb situació objectiu i actual

Finalment es presenta un gràfic de sectors, també en percentatges.

Il·lustració 9: Diagrama de sectors en percentatge

6-Pla de projectes amb propostes de millora

Arribats a aquest punt, coneixem ja l'estat de la seguretat en l'empresa i el nivell de compliment dels controls ISO. És el moment de plantejar projectes que millorin l'estat de la seguretat en l'organització.

La descripció de les millores proposades (projectes) hauran d'ajudar a mitigar el risc actual a l'organització i evolucionar el compliment ISO fins a un nivell adequat. Aquests projectes han de derivar-se dels resultats obtinguts del AARR d'acord amb les recomanacions associades a les vulnerabilitat identificades i l'anàlisi de compliment de la norma UNE ISO / IEC 27002.

Els projectes plantejats seran resultants d'agrupar un conjunt de recomanacions identificades en la fase d'anàlisi de riscos per facilitar la seva execució. S'incidirà no només en la millora en relació amb la gestió de la seguretat, sinó també en possibles beneficis col · laterals com ara l'optimització de recursos, millora en la gestió de processos i tecnologies presents en l'organització analitzada.

Els projectes s'han de quantificar econòmicament i planificar en el temps, establint terminis de consecució dels seus objectius (en general, curt, mitjà i llarg termini).

Addicionalment, s'han d'incloure en la planificació punts de control que permetin considerar realment la implementació del Pla Director com un procés de millora contínua.

És important remarcar que els projectes no s'han de limitar a l'àmbit de la tecnologia, sinó que poden (habitualment, han de) afectar els diferents àmbits (pe recursos humans, organització). Els projectes que s'aborden en aquests aspectes han també plantejar-se.

La proposta de projectes ha d'anar alineada amb una anàlisi del impacte sobre la seguretat. Això comporta, que la seva execució ens ha d'indicar com evoluciona el risc i el impacte de materialització, així com el nivell de compliment dels diferents dominis de la norma ISO 27002.

Amb tota probabilitat, l'objectiu ha de ser anar evolucionant cap a un nivell de maduresa optimitzat.

S'ha d'indicar de forma gràfica en un diagrama de radar l'evolució dels diferents dominis i el seu compliment abans i després de la realització dels diferents projectes.

6.1-Metodologia

Aquest exercici de **Gestió del Risc es basarà en l'estàndard ISO/IEC 27005:2008** [7] proporciona les orientacions per dur a terme la Gestió del Risc a una organització, i particularment, dona suport als requeriments d'un Sistema de Gestió Seguretat de la Informació (SGSI) en concordança amb l'estàndard ISO / IEC 27001.

La situació de partida d'aquest exercici es basa en el resultat la fase anterior d'aquest TFM, a on es va obtenir l'estat actual del risc de l'organització avaluada.

Amb aquesta informació, **l'objectiu** es planificar l'execució d'un Pla Director de Seguretat de la Informació, d'una durada de tres anys. Tota vegada que el nivell CMM3 s'ha definit a l'exercici anterior per tots els dominis que tinguin un grau de compliment dels seus controls d'entre el 50% i el 90%, es farà, també, l'exercici de **dur tots els dominis**, durant el primer any d'implantació del Pla Director de Seguretat de la Informació, com a mínim, al nivell **CMM3 Definit,** amb un nivell de compliment del 80%. Durant la segona fase d'aplicació del Pla Director (següents dos anys), s'intentarà arribar a nivell **CMM5 Optimitzat** amb un nivell de compliment del 95%.

Per aconseguir apropar els dominis a aquests objectius, s'haurà de reduir el risc aplicant diferents salvaguardes o contramesures als controls que formen cada domini.

Com a primera acció, s'actuarà sobre el controls que al **AARR** han produït una resposta negativa de compliment **(NO)** i revisant alguns controls que tenen un nivell de compliment PARCIALMENT.

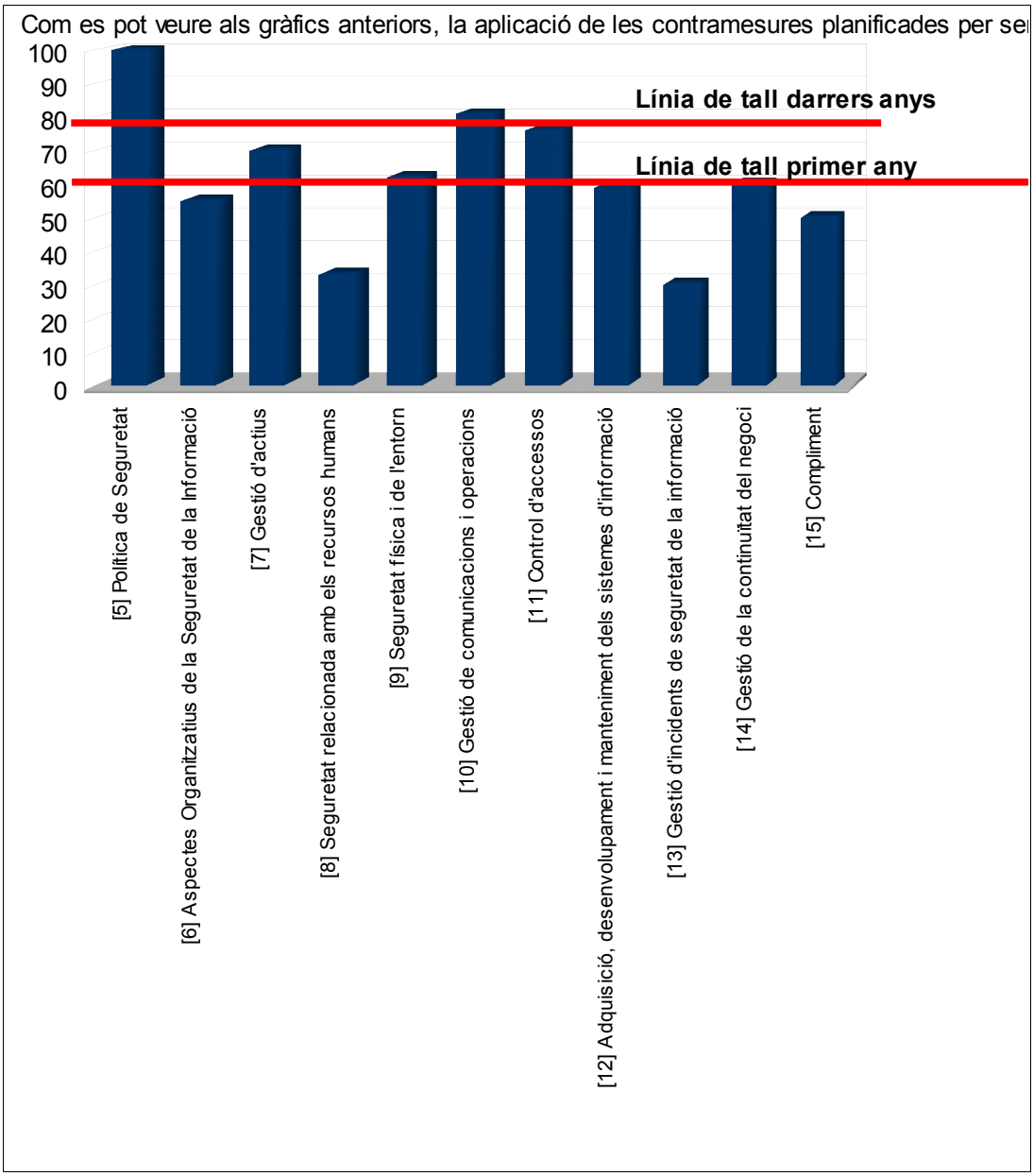
Hi ha diferents aspectes en els quals les salvaguardes actuen reduint el risc,

ja es parli dels controls ISO / IEC 27002:2005 o de qualsevol altre catàleg. Aquests són en general:

- Formalització de les pràctiques mitjançant documents escrits o aprovats.
- Política de personal.
- Sol · licituds tècniques (programari, maquinari o comunicacions).
- Seguretat física.

La protecció integral davant les possibles amenaces, requereix d'una combinació de salvaguardes sobre cada un d'aquests aspectes.

El següent diagrama de barres mostra la situació actual per cada domini de seguretat de la informació i la línia de tall que delimitarà els dominis sobre els que s'haurà d'actuar:



Com demostra el gràfic anterior, s'ha d'actuar a la pràctica totalitat dels dominis per dur-los al nivell L3 amb un percentatge mínim de compliment del 80%. Això durant el primer anys d'aplicació del Pla. Posteriorment caldrà incrementar el nivell de compliment per tal d'assolir o apropar-se a nivell CMM5 amb un nivell de compliment del 95%

6.2-Gestió de riscos

Amb aquest quadre de gestió de riscos es relacionaran les contramesures que permetran incrementar el nivell de compliment del domini a que afecten. Per cada control es proposaran un seguit de contramesures. Per cada una de les contramesures s'indicara:

- El cost d'implantació que representen, indicant:
  - A [Alt , mes de 30.000€]
  - M [Mitjà, entre 2.000 i 30.000 €]
  - B [Baix, menys de 2.000 €]
- El termini d'implantació, indicant:
  - L [Llag, mes de 12 mesos]
  - M [Mitjà, entre 6 i 12 mesos]
  - C [Curt, menys de 6 mesos]

En color verd s'han marcat aquelles contramesures que s'aplicaran durant el primer any d'implantació del Pla. Son contramesures de baix cost econòmic i de curta implantació en el temps, però son la base per la restà d'implantacions.

En color groc, s'han representen les contramesures que tenen un cost mitja o un termini mitjà d'implantació. Aquestes contramesures s'implantaran dintre del segon i tercer anys d'implantació del Pla.

En color blau, s'han identificat les contramesures amb un cost o temps d'implantació alt. Aquestes, junt amb les de color groc s'implantaran durant el segon i tercer any d'implantació del Pla.

En color vermell, aquells controls que s'ha d'assumir el risc, ja que,per situació de la tecnologia actual o del tipus de sistemes existent no es poden aplicar. En aquest cas, s'assumirà el risc, malgrat que en iteracions posteriors del Pla Director de Seguretat, s'haurà d'anar millorant.

En color gris, s'ha decidit que, en darrera instància, aquest control NO APLICA al negoci de NUCSSION.

#	Contramesures	Cost	Termini	ISO 27002		
1	S'han de redactar acords de confidencialitat per TOTS els empleats, contractistes i empreses col·laboradores. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	6	1	5
2	S'han d'establir acords de intercanvi amb la RESTA de Centrals d'aquest tipus per tal de millorar la cooperació i coordinació en temes de seguretat. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	6	1	7
3	S'ha de planificar la realització periòdica de revisions independents de la seguretat de la informació. Aquesta planificació ha de quedar recollida dins del document de Polítiques de Seguretat.	B	C	6	1	8
4	S'han de revisar i modificar TOTS els contractes i acords amb tercers per satisfer els requeriments de seguretat de 6.2.1. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	M	C	6	2	3
5	S'han de finalitzar les designacions els propietaris de la informació i dels actius associats amb els recursos per el seu tractament. Aquesta designació ha de quedar recollida, com annexe dins el document de Polítiques de Seguretat.	B	C	7	1	2
6	S'ha de comprovar la veracitat dels curricula presentats pels candidats a incorporar-se a la plantilla de l'empresa, confirmant les qualificacions acadèmiques i professionals al·legades. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	8	1	2
7	S'ha de MODIFICAR el model de contracte de relació laboral amb empleats i tercers perquè siguin acceptats i signats els termes i condicions dels seus contractes de treball, establint les seves responsabilitats i les de la organització en matèria de seguretat de la informació Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	8	1	3
8	S'ha d'incloure dins del document de Polítiques de Seguretat un apartat a on es faci menció a la responsabilitat de la Direcció en demanar als empleats, contractistes i tercers que apliquin la seguretat d'acord amb les polítiques i procediments establerts.	B	C	8	2	1

#	Contramesures	Cost	Termini	ISO 27002		
9	S'ha d'establir un procés disciplinari formal pels empleats que haguessin provocat algun incident de seguretat. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	8	2	3
10	S'ha de revisar el procediment de RRHH quant a la notificació de cessament o canvi per incloure, si s'escau, els requeriments de seguretat i les responsabilitats legals en curs. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	8	3	1
11	S'ha de prendre les mesures adients per evitar que en el CPD s'emmagatzemin materials perillosos o inflamables. Els suports de backup han de ser traslladats, immediatament després de finalitzar les operacions de copia, a un lloc segur fora del CPD. S'ha de disposar d'un armari ignifug de capacitat suficient per emmagatzemar el cicle complert de copies de seguretat. Aquests requeriments han de quedar recollits dins del document de Polítiques de Seguretat.	M	M	9	1	4
12	S'ha de prohibir i verificar que dins les àrees protegides no s'entren equips de fotografia, vídeo o àudio, malgrat es disposi de l'adient autorització. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	9	1	5
13	S'ha de revisar tot el material que es rep, abans de ser traslladat de-de les àrees de carrega i descarrega per tal d'evitar amenaces potencials. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	C	9	1	6
14	Tots els ordinadors portàtils propietat de l'empresa que hagin de sortir fora dels seus recintes han d'estar xifrats. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	A	M	9	2	5
15	S'ha de esborrar, de forma segura, la informació dels dispositius que es retirin com a obsolets (Pcs, portàtils, discos externs, dispositius USB). Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	M	M	9	2	6
16	El suports extractables s'han de gestionar com s'indica a aquest control. Aquest requeriment ha de quedar recollit, amb totes les recomanacions i bones pràctiques, dins del document de Polítiques de Seguretat.	B	B	10	7	1
17	El registre de logs de l'administrador de sistemes no es pot du a terme amb els sistemes actuals. La			10	10	4

#	Contramesures	Cost	Termini	ISO 27002		
	implantació d'aquest control representaria un cost molt superior al benefici que podria aportat. Existeixen mesures contractual i de revisions addicionals que permeten verificar el comportament honest de l'administrador de sistemes					
18	S'ha de redactar el procediment de revisió periòdica dels drets d'accés dels usuaris. S'ha de registrar la concessió/eliminació de drets d'accés cada vegada que es produeix. Aquests requeriments han de quedar recollits dins del document de Polítiques de Seguretat.	B	B	11	2	4
19	S'ha de redactar una política d'obligat compliment, de lloc de treball endreçat i pantalla neta. Aquesta passarà a formar part del document de Polítiques de Seguretat.	B	B	11	3	3
20	S'ha d'implantar el sistema de gestió de contrasenyes a les dos xarxes principals de la empresa. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	M	M	11	5	3
21	S'ha d'implantar un sistema de limitació de temps de connexió pels terminals que estableixen connexió directa amb l'ODP. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	M	M	11	5	6
22	S'ha d'aïllar la xarxa de SISTEMES (ODP) de la xarxa de GTEC, permeten, únicament, tràfic unidireccional entre la primera i la segona, fent impossible el tràfic en sentit contrari. Aquesta unidireccionalitat s'ha d'implementar, obligatòriament, amb un DATADIODE. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	A	L	11	6	2
23	S'ha de publicar un procediment d'obligat compliment, EXTENSIBLE als treballadors de l'empresa, contractistes i tercers que obligui que pels nous desenvolupaments o per la millora dels actuals, s'especifiquin els requisits dels controls de seguretat. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	B	B	12	1	1
24	La detecció de corrupció de dades no es pot du a terme amb els sistemes actuals. La implantació d'aquest			12	2	2

#	Contramesures	Cost	Termini	ISO 27002		
	control representaria un cost molt superior al benefici que podria aportat. Existeixen altres mesures tècniques i procedimental que permeten detectar aquestes situacions.					
25	La implantació del DATADIODE (veure #22) comportarà la necessitat de protegir la integritat dels missatges que arriben des-de la xarxa ODP fins a la xarxa GTEC. Per això serà necessari implantar un sistema de certificats digitals basat en una CA pròpia i interna de NUCSSION que podria requerir l'us d'un HSM. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	A	L	12	2	3
26	Com a conseqüència de #25 s'haurà d'establir una política d'usos criptogràfics. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	B	M	12	3	1
27	S'ha d'acabar d'assegurar que els entorns de desenvolupament treballin, únicament, amb dades de prova que no continguin informació sensible. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	A	L	12	4	2
28	S'ha d'establir un procediment, que haurà de formar part del document de Polítiques de Seguretat a on es descriguin les proves i els requeriments als fabricants sobre nou software adquirit per tal de detectar possibles portes del darrere i evitar fuites d'informació. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat.	M	M	12	5	4
29	S'ha d'acabar d'implantar normes d'aplicació als desenvolupaments externs per tal d'assegurar que els productes s'entreguen amb la qualitat i que compleixen amb els requeriments de seguretat exigits. S'han de revisar totes les entregues de desenvolupaments externs per complir amb les normes anteriors. Aquests requeriments han de quedar recollits dins del document de Polítiques de Seguretat	M	M	12	5	5
30	S'ha d'incloure un apartat de notificació d'esdeveniments de seguretat de la informació al Pla de Resposta a Incidents que ha de ser conegut per tots els empleats i contractistes. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	M	M	13	1	1
31	S'ha d'establir la obligatorietat contractual, tant per empleats com per a contractistes de anotar i notificar qualsevol punt dèbil que sigui observat o es sospiti que existeix en qualsevol dels sistemes d'informació de l'empresa. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	B	C	13	1	2

#	Contramesures	Cost	Termini	ISO 27002		
32	S'ha de redactar un procediment a on s'indiquin les accions a realitzar per tal de recopilar i preservar les proves i evidències quan s'hagi detectat un incident de seguretat. Aquesta recopilació es realitza per tal de complementar el procediment disciplinari de la empresa. Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	B	M	13	2	3
33	Per tal de suportat de forma adient la Gestió de la Continuïtat del Negoci s'ha d'iniciar un procés d'identificació dels esdeveniments que poden provocar interrupcions, així com la probabilitat de que es produeixin les interrupcions , els seus efectes i les conseqüències per la seguretat de la informació. Aquest procés haurà de quedar reflectit al document del Pla de Resposta a Incidents.	B	C	14	1	2
34	S'ha de redactar un procediment que permeti coordinar els Plans de Resposta a Incidents i de continuïtat de Negoci de les dos àrees fonamentals de que es composen els SI/TI de l'empresa (GESTIÓ/PROCÉS). Aquest requeriment ha de quedar recollit dins del document de Polítiques de Seguretat	B	C	14	1	4
35	S'ha de COMPLETAR el document de relació dels requeriments de seguretat TI del CSN amb els requeriments de seguretat de NUCSSION, per detectar possibles discrepàncies.	B	C	15	1	1
36	S'ha de FINALITZAR l'assegurament de la documentació crítica de l'organització, exportat, de forma xifrada, les copies de seguretat, tant del sistemes,dades i documents a una ubicació externa a la organització que compleixi amb les mesures de seguretat indicades per NUCSSION.	A	L	15	1	3
37	S'han d'instal·lar IDSs a les xarxes de GESTIÓ i PROCÉS per tal de monitoritzar l'us indegut dels sistemes d'informació..	M	M	15	1	5
38	S'ha decidit declarar la **NO APLICABILITAT** d'aquest control, ja que NUCSSION no realitza importació no exportació de software o hardware de xifrat.			15	1	6
39	S'a de redactar una norma que s'haurà d'incloure al document de Polítiques de Seguretat, a on els Directors hauran de revisar, periòdicament mitjançant un quadre de comandament, que s'estan complint les normes i polítiques de seguretat definides.	M	L	15	2	1

6.3-Pla Director de Seguretat

Després d'haver realitzat l'anàlisi de riscos s'han detectat una serie de millores que s'haurien d'introduir per incrementat la seguretat dels actius d'informació.

Tota vegada que l'esforç a realitzar implica moltes activitats de durada i dotació econòmica diferents, s'ha decidit afrontar la implantació del Pla Director de Seguretat com un projecte a tres anys.

Durant el primer any, la major part dels controls a implantar son els que tenen un cost baix **(B)** i un termini d'implantació inferior a sis mesos (**C**), que es correspon amb el grup de controls del quadre de gestió de riscos marcats en color verd,i que representa la implantació del 58% de les contramesures recomanades. Malgrat aquesta limitació, potser s'haurà d'incloure, dins d'aquesta fase, la implantació d'algun control que tingui una valoració econòmica més anta o una durada mes llarga, si es que algun dels controls implantats te alguna dependència que així ho requereixi.

L'objectiu d'aquesta primera implantació es dur el Sistema de Gestió de Seguretat a un nivell **CMM3** que representi un 80% de compliment.

Durant els dos anys següents, s'implantaran les contramesures que representin un const Mitja (**M**) o Alt (**A**) o las que tinguin un termini d'execució superior a sis mesos (**M** o **L**) colors groc i blau clar.

Amb la implantació d'aquest ultim seguit de contramesures s'espera apropar el sistema de Gestió de Seguretat de la Informació a **un nivell CMM5** que representi més del 95% de compliment.

La distribució de les tasques a realitzar es durà a terme en base a una distribució de tasques dividides en nou projectes. Els tres primer projectes es duran a terme durant el primer any d'implantació del Pla, mentre que el sis següents s'executaran durant els dos anys seguents.

6.3.1-Projectes a implantar durant el primer any

6.3.1.1-P1-Ampliació de la Política de Seguretat i dels marcs contractuals

Objectiu

Ampliar la Política de Seguretat de la Informació, amb l'objectiu de:

- Millorar la identificació de necessitats de seguretat i dels riscos informàtics als que s'enfronta l'empresa i les seves conseqüències.
- Ampliar la perspectiva de les regles i procediments que s'han d'implementar per afrontar nous riscos.
- Millorar el control i detecció de vulnerabilitats dels sistemes d'informació.
- Millorar la gestió de resposta a incidents.

Millorar els marcs contractuals amb els empleats, contractistes i tercers que prestin serveis a NUCSSION, incloent als respectius contractes l'establiment de les seves responsabilitats i les de la organització en matèria de seguretat de la informació

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

1, 2, 3, 4, 5, 6, 7, 8 ,9, 10, 16, 18, 19, 23, 31 , 32, 33, 34, 35

Termini d'execució

El termini d'execució es de **set mesos**.

Cost del projecte

El cost del projecte s'ha estimat en **30.000€** que es el cost d'un consultor especialista en polítiques de seguretat dedicat a part-time.

Tasques a desenvolupar

La tasca a desenvolupar per part del consultor serà la següent:

- Redactar tots els documents que indican les contramesures de cada un

dels controls de la relació de controls afectats.

- Modificar el document de Polítiques de Seguretat, incloent la nova normativa editada.
- Revisar tots els contractes actius actuals amb treballadors, contractistes i tercers per tal de proposar un nou redactat dels mateixos per que quedin alineats amb les noves exigències de les Polítiques de Seguretat.
- Després de vuit mesos, tornar a revisar l'estat des contractes per verificar que s'estan duent a terme les revisions anteriors incloent el clausulat corresponent.

6.3.1.2-P2-Millora de la Seguretat Física a les zones d'accés restringit i a les zones de carrega i descarrega

Objectiu

Evitar l'accés amb dispositius de gravació com càmeres e vídeo o fotografia a àrees d'accés restringit.

Revisar els materials que es reben en zones de carrega i descarrega per tal de garantir que no causaran cap problema quan siguin introduït en zones d'accés restringit.

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

12, 13

Termini d'execució

El termini d'execució es de **dos mesos.**

Cost del projecte

El cost del projecte s'ha estimat en **2.000€** que es el cost d'un formador amb experiència en seguretat.

Tasques a desenvolupar

La tasca a desenvolupar per part del formador serà la següent:

- Formar als vigilats de seguretat i als responsables de TI que tenen accés a àrees restringides de com detectat i notificar a Seguretat Física l'intent d'introducció de dispositius prohibits en àrees restringides.
- Formar als vigilants de seguretat per verificar que qualsevol tramesa rebuda a las àrees de carrega i descarrega que hagi d'anar a un àrea restringida s'ha d'haver revisat amb raigs X i amb detector d'explosius, a més de la corresponent inspecció visual.

6.3.1.3-P3-Gestió dels drets d'accés

Objectiu

Implantar el registre de la concessió / retirada dels drets d'accés a aplicacions i sistemes. Aquesta implantació incrementa el nivell de seguretat, al mateix temps que ho fa sobre el compliment derivat de Lleis com la LOPD

Controlar, de manera efectiva, qui disposa de permís d'accés par accedir a aplicacions i sistemes.

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

18

Termini d'execució

El termini d'execució es de **sis mesos.**

Cost del projecte

El cost del projecte s'ha estimat en **40.000€.**

L'import correspon al desenvolupament, implantació i explotació d'una eina de gestió software que utilitzaran els administradors de sistemes. Amb aquesta eina podran registrar tota l'activitat de concessió/retirada de credencials a usuaris per l'accés als sistemes i aplicacions.

El producte a lliurar pel desenvolupador ha de ser del tipus “claus en ma”, proporcionant el software, manual d'instal·lació, manuals d'us.

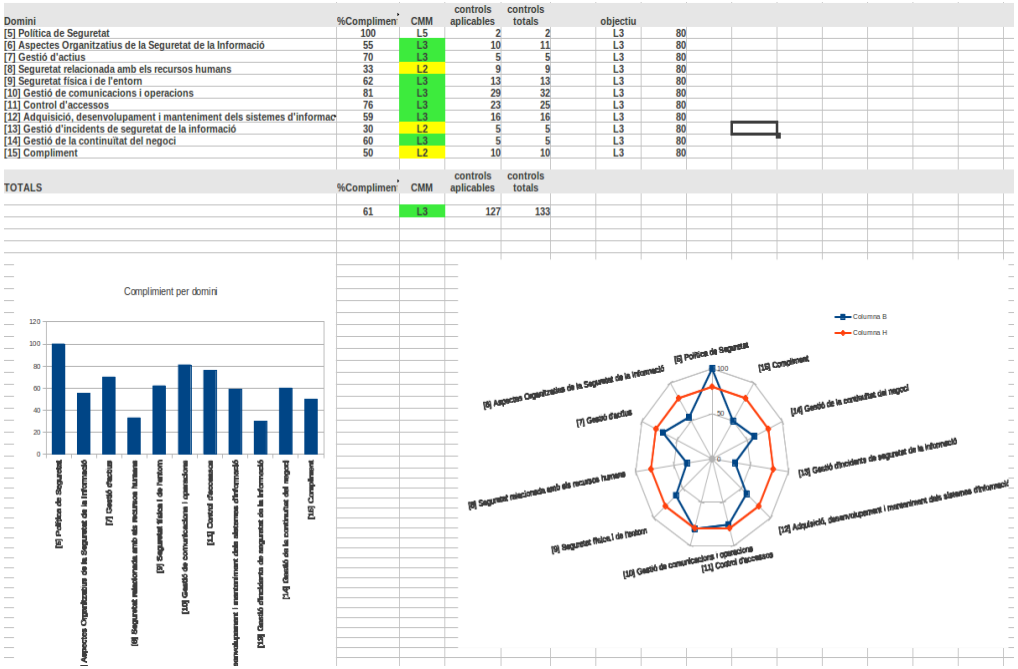
A banda de la eina, el desenvolupador haurà de dur a terme una formació presencial de vuit hores als administradors de sistemes que hagin d'utilitzar-la.

Tasques a desenvolupar

La tasca a desenvolupar per part del consultor serà la següent:

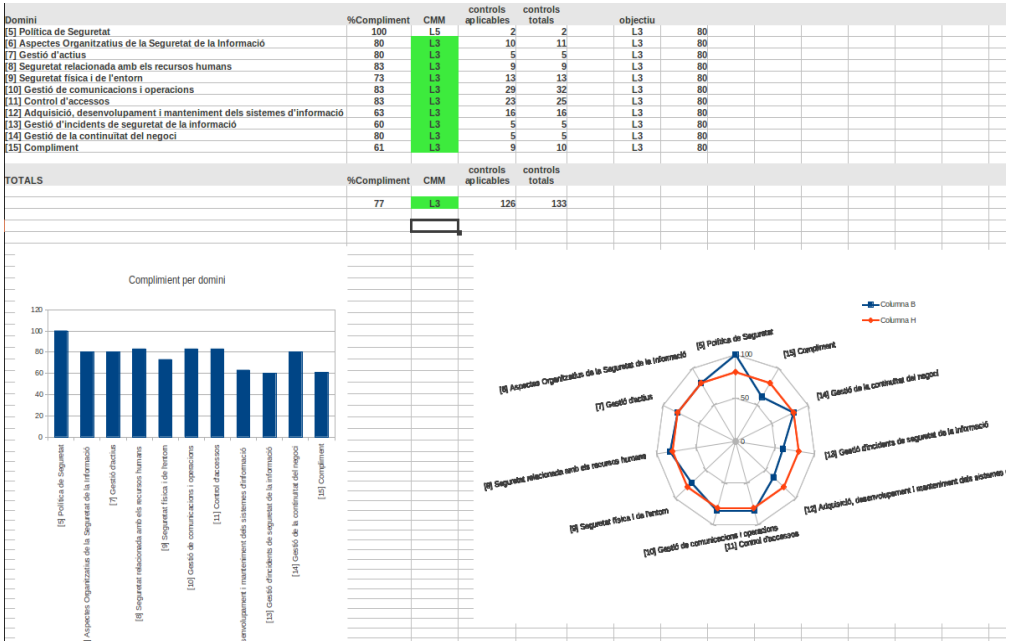
- Desenvolupament, instal·lació, formació i documentació del sistema esmentat.

6.3.1.4-Resultats comparatius després de la implantació de contramesures al primer any



Domini	%Compliment	CMM	controls aplicables	controls totals	objectiu	
[5] Política de Seguretat	100	L5	2	2	L3	80
[6] Aspectes Organitzatius de la Seguretat de la Informació	55	L3	10	11	L3	80
[7] Gestió d'actius	70	L3	5	5	L3	80
[8] Seguretat relacionada amb els recursos humans	33	L2	9	9	L3	80
[9] Seguretat física i de l'entorn	62	L3	13	13	L3	80
[10] Gestió de comunicacions i operacions	81	L3	29	32	L3	80
[11] Control d'accessos	76	L3	23	25	L3	80
[12] Adquisició, desenvolupament i manteniment dels sistemes d'informac	59	L3	16	16	L3	80
[13] Gestió d'incidents de seguretat de la informació	30	L2	5	5	L3	80
[14] Gestió de la continuïtat del negoci	60	L3	5	5	L3	80
[15] Compliment	50	L2	10	10	L3	80

TOTALS	%Compliment	CMM	controls aplicables	controls totals
	61	L3	127	133



Domini	%Compliment	CMM	controls aplicables	controls totals	objectiu	
[5] Política de Seguretat	100	L5	2	2	L3	80
[6] Aspectes Organitzatius de la Seguretat de la Informació	80	L3	10	11	L3	80
[7] Gestió d'actius	80	L3	5	5	L3	80
[8] Seguretat relacionada amb els recursos humans	83	L3	9	9	L3	80
[9] Seguretat física i de l'entorn	73	L3	13	13	L3	80
[10] Gestió de comunicacions i operacions	83	L3	29	32	L3	80
[11] Control d'accessos	83	L3	23	25	L3	80
[12] Adquisició, desenvolupament i manteniment dels sistemes d'informació	63	L3	16	16	L3	80
[13] Gestió d'incidents de seguretat de la informació	60	L3	5	5	L3	80
[14] Gestió de la continuïtat del negoci	80	L3	5	5	L3	80
[15] Compliment	61	L3	9	10	L3	80

TOTALS	%Compliment	CMM	controls aplicables	controls totals
	77	L3	126	133

Situació inicial, abans del primer any d'aplicació de control

Situació després d'aplicar els controls del primer any

els respectius fulls de calcul acompanyen a aquesta entrega

Inicial: RubioRodriguezEnrique_TFM_GestioDelRisc-inicial.ods

Primer any: RubioRodriguezEnrique_TFM_GestioDelRisc-primer-any.ods

6.3.1.5-Conclusions primer any aplicació contramesures

Com es pot veure als gràfics anteriors, la aplicació de les contramesures planificades per ser implantades durant el primer any, han aconseguit el seu objectiu i han dut tots els dominis al nivell de compliment CMM3. També s'ha aconseguit dur la majoria dels dominis a un nivell de compliment proper al 80%. Realment, com es pot veure a la gràfica de la dreta (si s'amplia una mica), el percentatge aconseguit aplicant molts controls de tipus organitzatius, dos de seguretat física i un de tècnic ha propiciat que s'aconseguís un 77% de compliment, de mitjana.

6.3.2-Projectes a implantar durant els següents dos anys

6.3.2.1-P4-Prevenció de l'un indegut dels recursos de tractament de la informació

Objectiu

Aquest projecte te com a objectiu el incrementar, notablement, les mesures de prevenció del us indegut dels recursos de tractament de la informació i el seguiment de possibles intents intents d'intrusió.

Amb aquest seguit de mesures es pretén:

- Millorar la identificació i autenticació d'usuaris als sistemes incrementant les exigències dels sistemes de gestió de contrasenyes.
- Limitar els temps de connexió desatesa de terminals de l'ODP
- Seguiment de tot el tràfic que circula per les xarxes de l'organització amb la intenció de detectar possibles intrusions i utilitzacions anormals dels sistemes de la empresa. Aquesta tasca es durà a terme mitjançant la implantació d'un IDS de Xarxa.

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

20, 21, 37

Termini d'execució

El termini màxim d'execució es de **vuit mesos** des de l'inici del projecte.

Cost del projecte

El cost del projecte s'ha estimat en **40.000€** que es correspon amb el següent:

- 24.000€ -Adquisició del hardware IDS - HP S660N Intrusion PreventionSystem-750Mbps-5x 10/100/1000BaseT copper and 5x 1Gb fiber segments.
- 5.000€ - configuració, fine tunning del dispositiu i formació d'explotació al equip de sistemes.
- 11.000€ - Tasques de suport a la configuració dels servidors LDAP i suport a usuaris per l'adaptació al nou sistema.

Tasques a desenvolupar

La relació de tasques a desenvolupar serà la següent:

- Licitar l'adquisició del hardware IDS i del servei de configuració amb els proveïdors habituals.
- Instal·lar i configurar l'IDS.
- Formar als administradors de sistemes en la configuració i explotació de l'IDS
- Configuració de les polítiques de contrasenyes als servidors LDAP de les xarxes de Gestió i Processos
- Suport a usuaris en el canvi inicial de contrasenyes i formació al CAU per atenció als usuaris en el canvi de contrasenyes.

6.3.2.2-P5-Millora en les Polítiques de Seguretat

Objectiu

Millorar les polítiques de seguretat incloent la obligatorietat de la comunicació i retroalimentació d'incidents de seguretat i incloure la revisió periòdica del compliment de les polítiques per part de la direcció mitjançant un quadre de comandament

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

30, 39

Termini d'execució

El termini d'execució es de **dotze mesos**.

Cost del projecte

El cost del projecte s'ha estimat en **50.000€** que es correspon amb el següent:

- 10.000€ - Desenvolupament a la intranet corporativa d'una plana de notificacions d'incidents de seguretat.
- 40.000€ - Desenvolupament d'un quadre de comandament per Direcció a on es farà el seguiment dels indicadors del compliment de les polítiques de seguretat

Tasques a desenvolupar

El recull de tasques a desenvolupar serà el següent:

- Desenvolupar, dins de la intranet corporativa, una plana web per que tots els treballadors de NUCSSION puguin reportar incidents de seguretat que s'hagin produït o les sospites de que es poden produir amb algun àmbit de la companyia. La informació per part dels treballadors ha de tenir la realimentació adient, informant als treballadors que han reportat un incident quan s'ha resolt.
- Desenvolupament d'un quadre de comandament per Direcció per realitzar el seguiment dels indicadors de compliment de polítiques de seguretat. Aquest quadre de comandament du aparellada la recollida de dades per poder explotar els indicadors.

6.3.2.3-P6-Millora de la seguretat del CPD i dels suports (backups i ordinadors portàtils)

Objectiu

Millorar la seguretat del CPD davant amenaces de foc, de la custodia de les copies de seguretat i de la informació dels portàtils i dispositius extraïbles (USB).

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

11, 14, 15, 36

Termini d'execució

El termini d'execució es de **dotze mesos**.

Cost del projecte

El cost del projecte s'ha estimat en **34.500€** que es correspon amb el següent:

- 24.000€ - Tres armaris ignífugs amb certificacions EN-1047-1 S 120 DIS i ECB-S C02
- 3,000€ - Instal·lació i ancoratge dels armaris al bunker de seguretat física
- 5,000€ - 50 Llicències de xifrat complert de portàtils
- 2,500€ - Software esborrat segur dades suports.

Tasques a desenvolupar

El recull de tasques a desenvolupar serà el següent:

- Licitació de la adquisició de tres armaris ignífugs amb certificacions EN-1047-1 S 120 DIS i ECB-S C02
- Instal·lació i ancoratge dels armaris al edifici de seguretat física dins del bunker d'arxiu.
- Licitació de 50 llicències de software de xifrat de disc de portàtils (crypt200 o similar).
- Instal·lació deli xifrat dels 40 portàtils que surten diàriament de la companyia.
- Instal·lació del software de esborrat segur als equips dels responsables de retirada de suports.
- Redacció del document d'esborrat segur a la retirada de suports
- Redacció del document d'instal·lació del xifrat als equips que ha de sortir de NUCSSION.
- Modificació del procediment de copies de seguretat per treure, immediatament, les copies del CPD i dur-les als nous armaris ignífugs.
- Redacció i supervisió del compliment de la norma que prohibirà que al CPS s'emmagatzemin productes inflamables o perillosos.

6.3.2.4-P7-Millora de la seguretat pel software comercial o el desenvolupat a mida

Objectiu

Millorar la seguretat del software comercial (productes tancats) o el desenvolupat a mida per NUCSSION, de tal manera que als contractes amb els fabricants o amb els desenvolupadors s'indiquin les condicions que haurà de superar el software per ser acceptat a les instal·lacions de NUCSSION. Amb aquestes millores es pretén evitar que el software adquirit per NUCSSION no presenti backdoors que podrien malmetre o provocar fuites d'informació sensible (recordar **Stuxnet**).

Aquesta millora significara una revisió de les entregues o la compra de productes tancats per tal d'assegurar que compleixen amb els requeriments de NUCSSION.

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

28, 29

Termini d'execució

El termini d'execució es de **dotze mesos** d'implantació i, posteriorment, procés continuu.

Cost del projecte

El cost del projecte s'ha estimat en **60.000€** que es correspon amb el següent:

- 60.000€ - Const de la incorporació d'un nou recurs al departament de TI per desenvolupar, únicament, tasques de validació de productes comercials i dels productes desenvolupats a mida de NUCSSION, abans de la seva acceptació per passar a producció.

Tasques a desenvolupar

El recull de tasques a desenvolupar serà el següent:

- Revisió de tot el software comercial o desenvolupat a mida, sobre l'entorn de proves de NUCSSION, per de validar el compliment dels requeriments de seguretat de NUCSSION. Per dur a terme aquestes valoracions s'utilitzaran mitjans com ara, analitzador de protocols, sniffers de xarxa, i qualsevol instrument a l'abast per tal de garantir que el software adquirit funciona segons les seves especificacions i no fuita cap tipus d'informació no autoritzada.

6.3.2.5-P8-Millora de l'entorn de desenvolupament de NUCSSION

Objectiu

Millorar la seguretat del entorn de desenvolupament de NUCSSION ja que, actualment , es treballa (encara que obsoletes) amb copies de dades reals que poden provocar una fuita important d'informació sensible que por repercutir en incompliments legals greus (LOPD i altres)

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

27

Termini d'execució

El termini d'execució es de **sis mesos**.

Cost del projecte

El cost del projecte s'ha estimat en **5,000€** que es correspon amb la compra d'un producte de Data Masking.

Tasques a desenvolupar

El recull de tasques a desenvolupar serà el següent:

- Licitació de la adquisició d'un producte de Data Masking (InfoSphere Optim Test Data Mgmt and Data Masking IBM)
- Instal·lació dins l'entorn adient del producte i proves d'extracció de les bases de dades REALS per carregar a les BBDD de desenvolupament
- Proves del manteniment de la integritat referencial a l'entorn de desenvolupament
- Posada en explotació per realitzar les actualitzacions periòdiques que demani el departament de desenvolupament.

6.3.2.6-P9-Aïllament físic de les xarxes de gestió i procés

Objectiu

Aïllar, físicament, les xarxes de gestió i procés, implantant un dispositiu que impedeixi, que es pugui arribar a la xarxa de procés des de la xarxa de gestió.

Aquest tipus d'impediment s'aconsegueix amb un data diode que només permet el pas d'informació en un sentit.

Aquest aïllament permetrà complir amb els requisits de defensa en profunditat que el Consell de Seguretat Nuclear (CSN) ha dictat en les seves darreres resolucions de protecció de les xarxes lògiques de les centrals nuclears.

Relació de controls afectats

La relació de controls afectats, segons la llista de Gestió de Riscos son:

22, 25, 26

Termini d'execució

El termini d'execució es de **vint-i-quatre mesos**.

Cost del projecte

El cost del projecte s'ha estimat en **90.000€** que es correspon amb el següent:

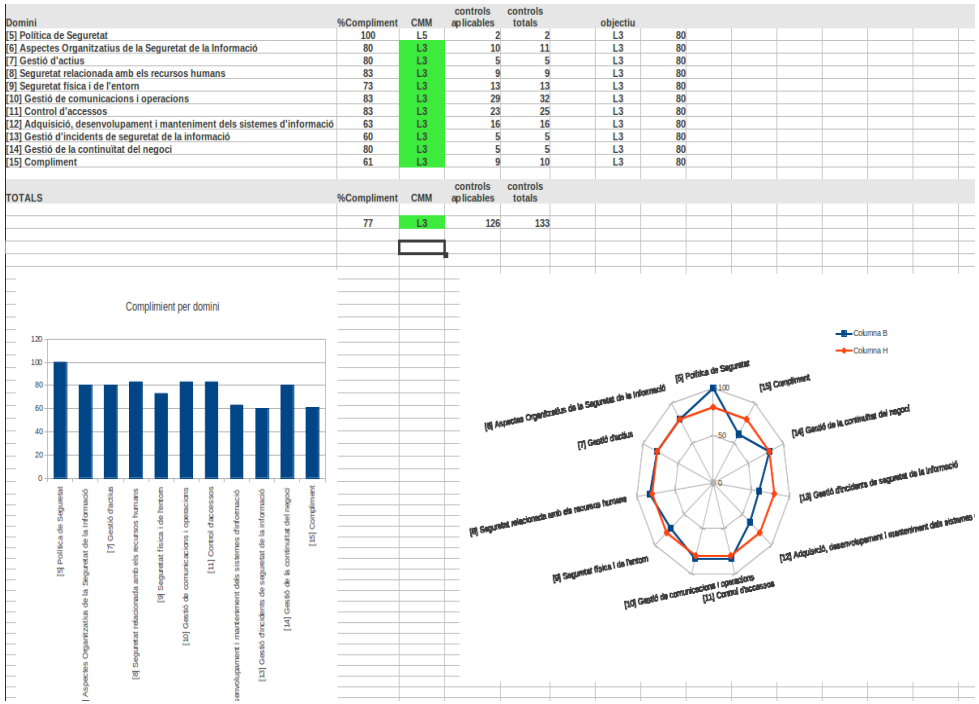
- 10.000€ - Licitació de la adquisició de dos dispositius físics (data-diode)
- 40,000€ - Software i servidors per suportar un arxiu de senyals de planta a dins la xarxa de gestió
- 40.000€ - Nou desenvolupament, amb inclusió d'autenticació de missatges, proves i validació dels processos de comunicació de dades entre la xarxa de procés i la xarxa de gestió

Tasques a desenvolupar

El recull de tasques a desenvolupar serà el següent:

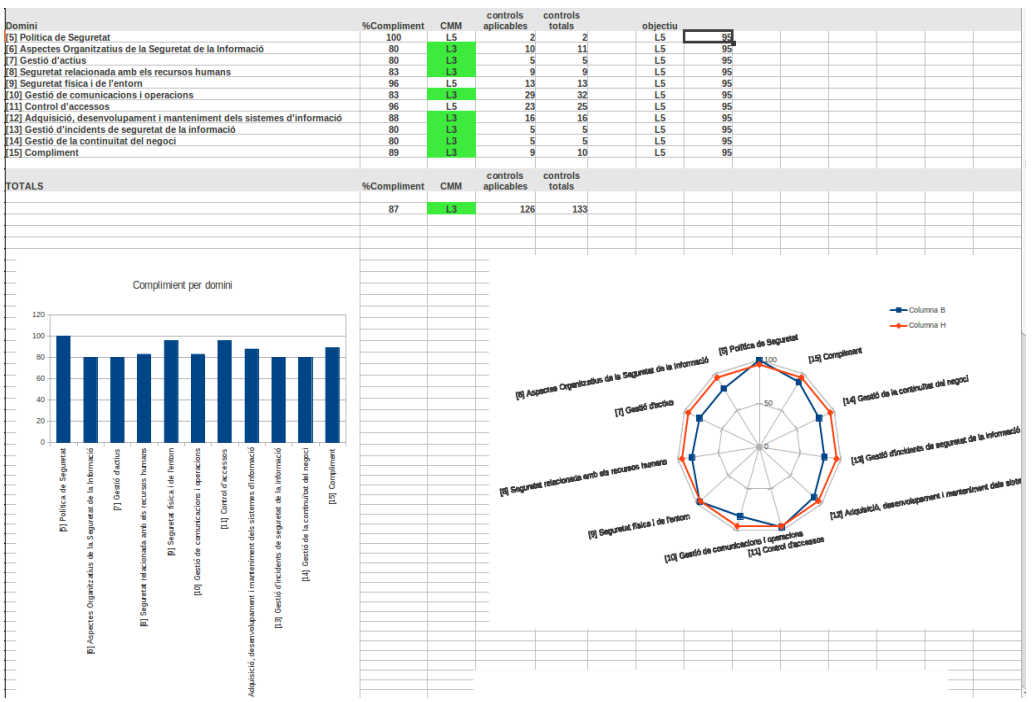
- Licitació de la adquisició dels data diode
- Licitació de la adquisició de dos servidor (cluster) per adquisició de senyals i arxiu.
- Licitació de la adquisició del software de gestió d'històrics de senyals de planta.
- Licitació de la adquisició del emmagatzematge per les senyals rebudes de l'ODP.
- Licitació del desenvolupament de les interfícies que permetin enviar les senyals de l'ordinador ODP cap a la xarxa de gestió, fent servir protocol UDP, amb validació de missatges.
- Instal·lacions del hardware
- Instal·lacions del software
- Proves i validació sense desconnexió del sistema actual, mantenint el dos sistemes en paral·lel.
- Posada en explotació de tot el projecte.

6.3.2.7-Resultats comparatius després de la implantació de contramesures als dos anys següents



Domini	%Compliment	CMM	controls aplicables	controls totals	objectiu	
[5] Política de Seguretat	100	L5	2	2	L3	80
[6] Aspectes Organitzatius de la Seguretat de la Informació	80	L3	10	11	L3	80
[7] Gestió d'actius	80	L3	5	5	L3	80
[8] Seguretat relacionada amb els recursos humans	83	L3	9	9	L3	80
[9] Seguretat física i de l'entorn	73	L3	13	13	L3	80
[10] Gestió de comunicacions i operacions	83	L3	29	32	L3	80
[11] Control d'accessos	83	L3	23	25	L3	80
[12] Adquisició, desenvolupament i manteniment dels sistemes d'informació	63	L3	16	16	L3	80
[13] Gestió d'incidents de seguretat de la informació	60	L3	5	5	L3	80
[14] Gestió de la continuïtat del negoci	80	L3	5	5	L3	80
[15] Compliment	61	L3	9	10	L3	80

TOTALS	%Compliment	CMM	controls aplicables	controls totals
	77	L3	126	133



Domini	%Compliment	CMM	controls aplicables	controls totals	objectiu	
[5] Política de Seguretat	100	L5	2	2	L5	95
[6] Aspectes Organitzatius de la Seguretat de la Informació	80	L3	10	11	L5	95
[7] Gestió d'actius	80	L3	5	5	L5	95
[8] Seguretat relacionada amb els recursos humans	83	L3	9	9	L5	95
[9] Seguretat física i de l'entorn	96	L5	13	13	L5	95
[10] Gestió de comunicacions i operacions	83	L3	29	32	L5	95
[11] Control d'accessos	96	L5	23	25	L5	95
[12] Adquisició, desenvolupament i manteniment dels sistemes d'informació	88	L3	16	16	L5	95
[13] Gestió d'incidents de seguretat de la informació	80	L3	5	5	L5	95
[14] Gestió de la continuïtat del negoci	80	L3	5	5	L5	95
[15] Compliment	89	L3	9	10	L5	95

TOTALS	%Compliment	CMM	controls aplicables	controls totals
	87	L3	126	133

Situació de partida segon any d'aplicació de les contramesures

Situació després d'aplicar els darrers contramesures durant els anys següents

els respectius fulls de calcul acompanyen a aquesta entrega

Primer any: RubioRodriguezEnrique_TFM_Fase5-GestioDelRisc-primer-any.ods

Dos darrers anys: RubioRodriguezEnrique_TFM_Fase5-GestioDelRisc-seguents-dos-anys.ods

6.3.2.8-Conclusions aplicació darreres contramesures

Com es pot veure als gràfics anteriors, la aplicació de les contramesures planificades per els darrers dos anys d'implantació del Pla Director de Seguretat de la Informació, han aconseguit l'objectiu d'apropar dos dimensions mes al nivell CMM5, però encara queda un camí llarg per recórrer a la recerca de l'excel·lència.

Aquest camí s'haurà d'anar assolint mitjançant un proces de millora continua (PDCA) basat en la revisió periòdica del Pla o cada vegada que s'implanti un canvi significatiu.

Cal destacar que durant el primer any, l'objectiu es CMM3 amb un 80% però pels darrers dos anys d'implantació del Pla, s'ha marcar un objectiu de CMM5 amb un nivell de compliment del 95%. Es per aquest motiu, que la gràfica de radar dels dos darrers anys pot semblar quasi igual que la del primer any, però els objectius percentuals son, clarament diferents.

L'èxit fonamental d'aplicació d'aquest Pla director, ha estat, incrementar notablement el nivell de seguretat dels sistemes d'informació de NUCSSION i el compliment exigit pel regulador (CSN) quant a la implantació d'una política de defensa en profunditat basada en la utilització de dispositius unidireccionals.

Finalment, l'esforç total, ha estat de tres anys i 351.500€. Cap recordar que una sanció per incompliment greu de LOPD pot anar de 300.000 a 500.000€ amb el que la inversió, que no només millora el compliment LOPD, sinó que alinea la seguretat de les TI amb el negoci, cal considerar que ha estat mes que raonable.

7-Canvis organitzatius

El Pla Director de la Seguretat de la Informació (PDS) de NUCSSION determina la següent estructura organitzativa quant a seguretat de la informació:

ROLS	Funcions i responsabilitats
Comitè de seguiment del pla	Estarà format pel Director General i pels Directors de cada àrea de l'organització (enginyeria, central, RRHH, finances) i supervisara totes les iniciatives i accions de seguretat
Responsable de seguretat de la informació (CISO)	Màxim responsable de la unitat de seguretat de la informació. Encarregat de coordinar i controlar les mesures de seguretat aplicables als sistemes d'informació. Reporta directament al comitè de seguiment del pla. Serà el responsable de dur a terme la implantació del PDS.
Responsable de seguretat TIC	Màxim responsable de seguretat del departament TIC (gestió). Supervisa, controla i administra els sistemes d'informació del seu àmbit, seguint les polítiques de seguretat de la organització, reportant els incidents de seguretat al CISO i coordinant amb el mateix CISO les intervencions a dur a terme en cas que es produís un incident de seguretat
Responsable de seguretat SDP	Màxim responsable de seguretat del departament SDP (proces). Supervisa, controla i administra els sistemes d'informació del seu àmbit, seguint les polítiques de seguretat de la organització, reportant els incidents de seguretat al CISO i coordinant amb el mateix CISO les intervencions a dur a terme en cas que es produís un incident de seguretat
Assessors externs	Organitzacions externes, especialitzades en seguretat, que col·laboraran en la implantació del PDS

Tots els càrrecs hauran de ser nomenats per la Direcció abans d'escometre aquest **PDSI.**

8-Annexes

8.1-Annexe I

Actiu			
Impacte	**acrònim**	**Valor**	**Descripció impacte**
Autenticitat			
DA-Desconeixement autor			
Confidencialitat			
RI-Revelació a interns			
RE-Revelació a externs			
Integritat			
EPE-Error petita escala			
EGE-Error gran escala			
MD-Modificació deliberada			
Disponibilitat			
15m-15 minuts			
3h-3 hores			
1d-1 dia			
1s-1 setmana			
DP-Destrucció parcial			
DT-Destrucció Total			
Traçabilitat			
TS-Desconeixement a qui se presta el servei			
TA-Desconeixement de qui accedeix o manipula dades			

Taula 15: Qüestionari valoració actius

9-Bibliografia

[1] Millora dels processos del programari amb CMMI

http://www.anella.cat/web/tic/articles_inno_emp/-/journal_articles/view/62_INSTANCE_OtWf/25818881/articlesInnovacioEmpresarial/1.0/27320369-_-millora_dels_processos_de_programari_amb_cmmi_oportunitats_i_experiencies_dins_del_plan_avanz_ca_ES_

[2] MAGERIT - Metodologìa

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

[3] MAGERIT Llibre III "Guías Técnicas" (apartat 2.1)

http://administracionelectronica.gob.es/recursos/PAE_12874011639808880.pdf?iniciativa=184

[4] MAGERIT Llibre II "Catálogo de elementos" (apartat 5)

http://administracionelectronica.gob.es/recursos/PAE_12874011419151767.pdf?iniciativa=184

[5] MAGERIT Llibre I "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" (pag 132)

http://administracionelectronica.gob.es/recursos/PAE_12874011156227961.pdf?iniciativa=184

[6] ISO/IEC 27002:2005 Guia de bones pràctiques

http://es.wikipedia.org/wiki/ISO/IEC_17799

[7] ISO/IEC 27005:2008 Directrius per a la gestió del risc

http://www.iso27000.es/download/doc_iso27000_all.pdf