Sistemes de Gestió de la Seguretat de la Informació

Treball Final de Màster (TFM 2013-2014)

Màster Interuniversitari en Seguretat de les TIC (MISTIC)

Memòria Final

Tutor: Arsenio Tortajada Gallego
Alumne: Jordi Miró Amigó
Data: Gener de 2014

"Ensenyar als nens l'ús del programari lliure a les escoles,
formarà individus amb sentit de llibertat"
Richard Stallman.

Autor del projecte: Jordi Miró Amigó, 2014

Agraïments:

Amb aquestes línies voldria agrair, primerament l'ajuda del consultor i tutor de la Universitat Oberta de Catalunya, que amb els seus comentaris de les diferents entregues parcials ha permès que s'hagi pogut completar el projecte i dissenyar una documentació final atractiva, i completa.

També voldria fer extensiu aquest agraïment a la meva família, que amb la seva gran paciència i comprensió han ajudat a que durant aquests mesos pogués dedicar el màxim temps possible a finalitzar aquest projecte del màster MISTIC.

Resum inicial:

Català:

El projecte exposat en aquest document és el TFM (Treball Final de Màster) del màster "MISTIC" (Màster Inter-universitari de Seguretat de Tecnologies de la Informació i de les Comunicacions), amb l'objectiu d'analitzar i estudiar l'estat dels sistemes de seguretat d'una organització, per poder crear les diferents descripcions de les tasques i fases d'un Sistema de Gestió de la Seguretat en aquesta empresa o organització.

Castellano:

El proyecto expuesto en este documento es el TFM (Trabajo de Final de Máster) del máster "MISTIC" (Máster Inter-universitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones), con el objetivo de analizar y estudiar el estado de los sistemas de seguridad de una organización, para poder crear las diferentes descripciones de los procesos y fases de un Sistema de Gestión de la Seguridad en esta empresa u organización.

English:

The project exposed in this document is the TFM of the "MISTIC" (Inter-university Security in Information Technology and Communications Master's Degree), has the aim of analysis and study the current systems security state of the organization, in order to cover and create the different descriptions of the tasks and phases of the ISMS (Information Security Management System) in this particular company or organization.

INDEX

1.FASE I - Situació actual, contextualització, objectius i anàlisis diferencial:

1.1.Introducció al projecte:

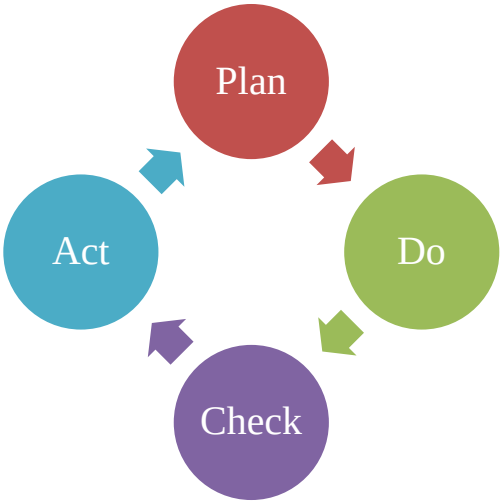
En el present projecte hem de tenir en compte que el principal objectiu és l'anàlisi de l'estat de seguretat dels sistemes d'informació d'una empresa, per poder-ne detectar les possibles amenaces, riscos i poder crear projectes que ajudin a millorar els possibles problemes o vulnerabilitats que existeixin en l'organització o empresa estudiada, tot tenint en compte el compliment del marc legal vigent.

Cal tenir en compte que actualment en una organització o empresa qualsevol es disposa de grans quantitats d'informació en diferents mitjans i en diferents ubicacions, una gran quantitat d'informació que és primordial per qualsevol empresa i per tant que vol conservar amb les màximes garanties que aquesta informació podrà ser consultada en qualsevol moment amb gran disponibilitat per tots els treballadors de l'empresa, al mateix temps, garantint-ne una màxima seguretat, perquè aquesta informació no pugui ser consultada per terceres parts no autoritzades.

Actualment ja és comencen a parlar en moltes organitzacions i empreses, amb forta utilització de les xarxes socials, del concepte de Big-Data, un concepte molt important i que anirà guanyant importància per les organitzacions en un futur molt pròxim. Ja que les organitzacions han de poder tractar grans quantitats d'informació que es genera a la xarxa i que poden esdevenir clau per poder guanyar mercat o poder augmentar les vendes o els clients potencials. Així mateix aquesta immensa quantitat de dades necessita una infraestructura forta i ben planificada que permeti el seu tractament eficaçment.

Per tot això, les organitzacions cada vegada més necessiten poder tenir un marc de gestió on recolzar els seus sistemes d'informació, es aquí on ens poden ajudar les normatives ISO, que ens permeten disposar d'un conjunt d'estàndards que són fàcilment consultables, i que és poden implantar en les nostres organitzacions per guanyar en eficàcia, i fins i tot reduint costs dels processos o dels elements de seguretat de que disposem, augmentant el rendiment, i per tant la millora de l'empresa, i de la seva reputació exterior.

En el projecte podrem veure la creació de les bases d'un pla director de seguretat, que conforma un element primordial amb el que ha de treballar l'organització i els seus responsables. Realment, constitueix un element clau alhora de planificar els projectes i millores de seguretat a aplicar a l'empresa en un futur pròxim o llunyà. Com en tota bona empresa es seguirà un procés de millora contínua, o com també s'anomena, PDCA (Plan-Do-Check-Act), que ens permetrà anar millorant els processos i tasques cíclicament.



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

- Estudiar la situació actual de l'empresa tractada.
- Identificar les amenaces que l'organització o que l'empresa té o hi està exposada, així com el seu impacte present i futur.
- Inventariar els actius de l'empresa, realitzant un inventari acurat i específic per cada tipologia d'actiu.
- Documentar la normativa de seguretat de la informació de que es disposa.
- Descriure el riscos de l'organització en els diferents elements.
- Proposar accions i projectes a realitzar per arreglar possibles problemes, avaluant el seu impacte un cop realitzada l'acció.
- Oferir els resultats de les accions i projectes proposats i realitzats, per obtenir-ne conclusions rellevants.

1.2.Enfoc i selecció de l'empresa:

1.2.1.Descripció inicial del negoci de l'empresa:

Per raons de confidencialitat algunes dades de seguretat analitzades, i el propi nom de l'empresa no podran ser revelats en aquest projecte, ja que podrien comprometre la seva seguretat, i confidencialitat de les dades, la seva informació tractada, les infraestructures de que disposen i la seguretat dels propis treballadors, en el cas que s'utilitzessin aquestes dades per atacar alguna vulnerabilitat detectada en el projecte actual.

L'empresa seleccionada es dedica a oferir diversos serveis immobiliaris a través d'Internet. El seu principal punt fort és el portal web, juntament amb una aplicació mòbil que permet un conjunt d'accions que tot seguit s'especifiquen breument.

El portal web, juntament amb l'aplicació per mòbil i tauletes Android, inclou funcionalitats de xarxa social col·laborativa (missatges, comentaris, tags, puntuacions) que els diferents usuaris poden utilitzar per poder tenir un control de les seves propietats immobiliàries. Aquests usuaris poden tenir un lloc virtual on veure organitzats els seus patrimonis (cases, pisos, locals, terrenys, pàrquings, segones residencies...), amb la informació rellevant de cadascuna, fotos, vídeos, documentació legal, d'urbanisme, entre d'altres, i pensant en que poden estar llogats, sense utilització, o per ús del mateix propietari. Així mateix aquestes propietats també poden posar-se en el mercat de lloguer o venda, entre els usuaris registrats i no registrats.

L'empresa destina els seus productes a un públic no expert, tipus usuari particular, no adreçat a API's ni a professionals del sector. No obstant últimament s'està pensant en adaptar-la per l'ús dels serveis en ajuntaments de pobles petits i organismes públics.

L'empresa utilitza les aplicacions per generar negoci, tenint la major part de serveis o seccions gratuïtes per atraure públic, però amb la combinació d'apartats o funcionalitats de pagament o serveis "Premium", que augmenten les possibilitats, la capacitat o les funcionalitats de l'aplicació, segons la contractació desitjada realitzada.

1.2.2. Organigrama del personal de l'empresa:

Els treballadors que formen part d'aquesta empresa estan formats per una sèrie de perfils de treballadors, entre els que podem destacar els següents:

- Direcció General, té assignat el rol de control dels diferents departaments de l'empresa, i de prendre les decisions estratègiques per l'empresa. En aquest cas la direcció està formada per dues persones.

- Departament de Comptabilitat i Finances, s'encarrega en el back-office de realitzar tota la gestió de les finances de l'empresa. Les administratives de comptabilitat i finances s'encarreguen de dur a terme totes les tasques administratives del departament.

- Departament de Màrqueting, s'encarrega de realitzar totes les gestions i funcions de promoció, descomptes a certs usuaris, i gestió de les campanyes a les xarxes socials, per promocionar els diferents serveis de que l'empresa disposa. Els comercials s'encarreguen de realitzar totes aquestes tasques de màrqueting i de gestió de clients del departament de màrqueting.

- Departament TIC (Tecnologies de la Informació i les Comunicacions), és on treballen els administradors TIC del portal web i de l'aplicació mòbil i que realitzen totes les tasques tècniques i de manteniment i millora del sistema i de la infraestructura.

- Departament d'Atenció a l'Usuari, és on es rep el feedback dels usuaris que tenen serveis contractats amb l'empresa. Podríem dir que és el call-center de l'empresa.

- Departament de RRHH (Recursos Humans), on es gestionen totes les tasques relacionades amb els recursos humans de l'empresa, contractacions, baixes...

- Departament de Desenvolupaments, on és realitzen les diferents modificacions, millores i desenvolupaments dels productes que l'empresa ofereix als seus usuaris (portal web i aplicació mòbil).

- Proveïdors: són els encarregats de realitzar tasques subcontractades per l'empresa, en el cas que aquestes siguin necessàries en algun moment.

- Personal de recepció i seguretat: són els encarregats de controlar la seguretat física i personal dels accessos, la recepció, i del interior i exterior de les instal·lacions de l'empresa.

- Usuaris del portal web i de l'aplicació mòbil, encara que no formen part de l'empresa, és pot considerar un perfil que interacciona amb els productes finals

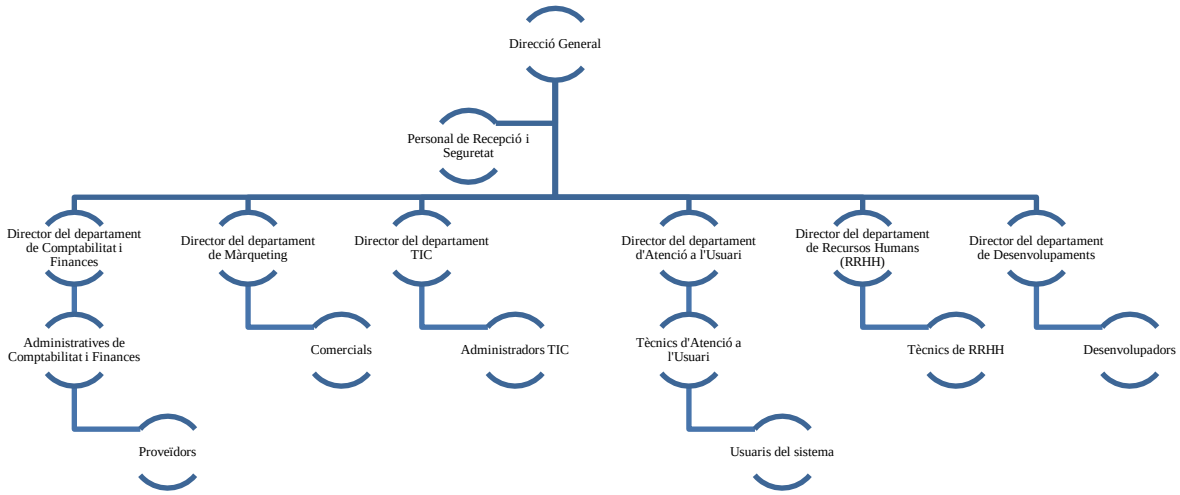
desenvolupats per l'empresa a través del portal web i de l'aplicació mòbil, com usuaris registrats gratuïts, usuaris no registrats, i usuaris registrats Premium.

- Els usuaris no registrats, són usuaris del portal web o de l'aplicació mòbil que només podrà realitzar les accions assignades als usuaris que només visiten la web i no estan registrats en el sistema.

- Els usuaris registrats gratuïts, són usuaris del portal web o de l'aplicació mòbil només podrà realitzar les accions assignades segons els seus rols, en aquest cas es tracta de usuaris que utilitzen els serveis gratuïts per usuaris registrats.

- Els usuaris registrats Premium, són els usuaris del portal web o de l'aplicació mòbil només podran realitzar les accions assignades segons els seus rols, en aquest cas es tracta d'usuaris que utilitzen tant els serveis gratuïts, com també tenen contractats serveis Premium.

Tot seguit podem veure un petit diagrama que resumeix de forma breu la principal organització dels empleats de l'empresa que s'han comentat en el punt anterior:



1.2.3. Infraestructura i funcionament de l'empresa:

Primerament, podem dir que actualment aquesta empresa no disposa d'un departament de seguretat específic, sinó que la seguretat forma part del departament TIC, que vetlla per garantir la seguretat diària de l'empresa, a part d'altres tasques pròpies del departament (per tant, no es centren en exclusivitat en les tasques de seguretat).

Els diferents perfils d'empleats de l'empresa disposen d'uns equips de sobretaula (HP Compaq Pro 6300 All-in-One), equips portàtils (Asus 15,6" 856CM Intel i5 3317U) i dispositius smartphones (Samsung S3 i S4) per dur a terme les seves tasques diàries a l'empresa, que en la majoria de casos, ells mateixos administren.

Els sistemes tenen un departament informàtic que realitza el manteniment periòdic dels sistemes, però de totes formes els equips dels empleats necessitarien millorar molt la

freqüència de les actualitzacions dels equips, ja que no existeix una política clara que indiqui les diferents pautes a seguir en cada cas.

L'entorn de millora i producció de les aplicacions disposen d'equips i entorns virtualitzats per a poder realitzar el desenvolupament i les diferents proves, i que són administrats per l'equip del departament d'informàtica, amb l'assignació dels diferents permisos.

El diferent programari dels equips de sobretaula i servidors és instal·lat pel departament d'informàtica, de totes formes, en els equips personals no es pot assegurar que els empleats no instal·lin pel seu compte altres programaris no autoritzats.

Tots els equips disposen del programari amb llicencia legal, per exemple, els sistemes operatius pels servidors (Windows Server 2012 i Linux Ubuntu Server), els sistemes operatius dels equips personals (Windows 7 i Linux Ubuntu 13.04), els processadors de texts (Microsoft Office Professional 2013), antivirus (McAfee SaaS Total Protection), així com algun sistema disposa de llicencies de programari lliure (LibreOffice).

La pàgina web de l'empresa esta desenvolupada en llenguatge HTML, PHP, i Java, i utilitza un domini .cat, ja que l'idioma principal de l'aplicació és el català, així com també es disposa dels idiomes complementaris de castellà i anglès.

L'empresa disposa d'una infraestructura de servidors i emmagatzematge pròpia, perquè es considera que això li aporta una major seguretat en les seves dades, al no disposar de terceres parts subcontractades.

Primerament, la tipologia de la xarxa interna, és una tipologia d'estrella, i diferenciant les connexions que els usuaris exteriors poden fer a la xarxa externa per consultar el portal web, de les connexions que fan servir els empleats de l'empresa en la xarxa interna. Si algun empleat, vol connectar-se a la xarxa interna des de l'exterior, es preveu un sistema de VPN per IP. Així com també es disposa de connexions Wifi protegides pels empleats que treballin amb els seus equips portàtils dins l'empresa. Així mateix la xarxa disposa dels estàndards de Gigabit Ethernet, per oferir el màxim de capacitats de la xarxa.
En la xarxa interna, l'empresa disposa d'un control dels nombres d'usuaris que s'hi poden connectar, i en casos de que hi hagi molta carrega d'usuaris alhora, podent-los desviar a servidors replicats menys carregats i que disposin dels mateixos serveis.

En les connexions dels usuaris del portal web i de l'aplicació mòbil, es disposa d'una infraestructura de servidors amb un sistema de balanceig, ja que d'aquesta manera, amb la utilització de balancejadors es poden desviar connexions d'usuaris a servidors menys carregats, i per tant, s'augmenta la fiabilitat del sistema i la satisfacció dels usuaris que l'utilitzin, evitant possibles problemes amb puntes d'usuaris connectats.

A part dels servidors físics, la infraestructura també disposa de virtualització de servidors, que ens permet augmentar les capacitats del sistema, ja que un sol equip pot funcionar com si fossin múltiples servidors, amb els avantatges que això suposa per la infraestructura.

La virtualització de servidors ens permet una sèrie d'avantatges, com pot ser el fet que aprofitem molt millor les capacitats de les màquines del sistema, ja que uns servidors físics poden estar molt desaprofitats, en canvi amb la virtualització es redueix el personal de manteniment necessari, l'espai ocupat pels servidors, els kilowatts d'energia gastats, i fins i tot la temperatura despresa per les diferents màquines.

Aquestes xarxes preveuen una seguretat, podent registrar i filtrar tot el transit que entri i surti de la xarxa de l'empresa. A més l'empresa disposa d'un conjunt de tallafocs que permeten evitar qualsevol intrusió o sortida d'informació no desitjada, ja sigui una fuga d'informació intencionada o no.

Com a maquinari, podem dir que el conjunt de servidors de la infraestructura estan aïllats i protegits en una sala de servidors (CPD), amb diferents elements de la xarxa de comunicacions, i amb elements de seguretat, com poden ser tallafocs, antivirus, anti-malware.

De maquinari també en podem trobar dels diferents equips personals del personal de l'empresa, o els diferents perifèrics que poden utilitzar els empleats de l'empresa, com poden ser escàners departamentals (HP ScanJet Enterprise 8500 fn1), impressores departamentals (HP LaserJet Enterprise 700 MFP), projectors departamentals (Toshiba TDPP8EU), i pissarres digitals per realitzar reunions (Smart Board SB680), entre d'altres.

La infraestructura utilitza un gestor documental–ECM de la casa Oracle, i dins la infraestructura tecnològica de l'empresa es té en compte que els empleats puguin disposar d'un equipament que els hi permet la captura de documents, per poder realitzar una gestió documental completa, i per tant, poder convertir el paper a documents digitals, més fàcilment organitzables, i consultables, per tant, com a infraestructura tecnològica, s'utilitza un element d'escanejat que permet convertir-ho en un procés automatitzat, ja que qualsevol document es pot capturar, guardar en el repositori i queda disponible per futures consultes.

Tots els elements de la infraestructura tecnològica necessiten protecció, però potser un dels elements més delicats és la sala on hi ha els diferents servidors (físics i virtuals), ja que un canvi de temperatura, o una humitat, pot provocar un mal funcionament de l'equipament. Per tant, en aquesta sala s'utilitzen sensors de temperatura, sensors d'humitat, sensors de moviment, i sistemes industrials d'aire condicionat per fer baixar la temperatura dels servidors, així com sistemes d'alarmes, que activen avisos a la xarxa quant detecten algun problema o intrusió.

Així mateix, també podríem pensar que en un futur podríem instal·lar sistemes redundants d'energia elèctrica, per evitar caigudes del sistema si ens quedem sense energia, per una tempesta, per exemple, ja que actualment el sistema només disposa d'un sistema SAI que dona energia durant un curt espai de temps.

Es disposa de servidors diferenciats per realitzar diferents tipus de tasques, com per exemple, servidors de bases de dades, servidors web, servidors d'aplicacions, així com també s'opta per virtualitzar algun servidor, per aprofitar més eficientment els recursos de les màquines, i recuperar-nos millor en cas d'una fallada del sistema.

De totes formes, seria important poder realitzar una millor redundància de servidors, i que aquests siguin el suficient escalables, per poder absorbir les necessitats de l'empresa. Pel que fa a la major redundància, ajudaria que un possible error no arribi al usuari final, i sigui més fàcilment reparable pel administrador que porta el registre d'incidències.

El sistema també disposa d'un sistema de còpies de seguretat i d'un sistema d'emmagatzematge d'informació (NAS/SAN) adequat per poder guardar totes les dades tant dels usuaris, com de la mateixa empresa.

Pel que fa referència a les bases de dades generals, es disposa de dos principals ben diferenciades, una per l'ús intern de l'organització, i una altra pels serveis dels diferents usuaris del portal web.

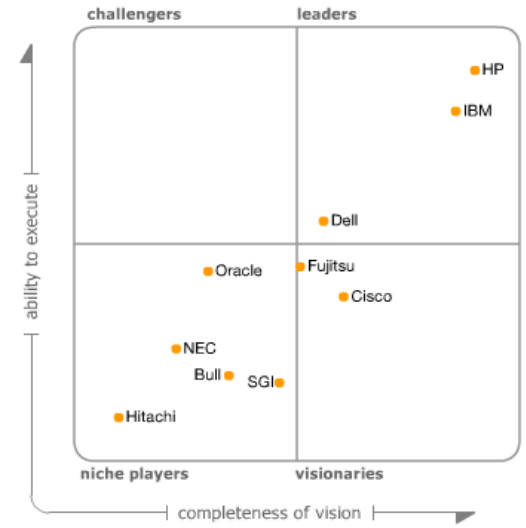
En el conjunt de servidors de l'empresa podem trobar el servidor on s'allotja la pàgina web i l'aplicació mòbil i la base de dades del programari dels usuaris, així com també disposa de servidors de correu i servidors interns per les aplicacions i les bases de dades, d'impressió, així com també de LDAP pels empleats.

L'empresa alhora de crear el seu propi CPD, va consultar els quadres de Gartner per poder realitzar la millor elecció, amb els fabricants més idonis en el seu moment. Tenint en compte elements molt importants de la infraestructura com són, els servidors, l'espai físic, la connectivitat, la refrigeració, i alguns dels sistemes punters de seguretat.

Si detallem una mica més quines solucions concretes es van utilitzar per la infraestructura, primerament cal veure el quadre de solucions LAN, podem veure que les empreses líders del mercat són, com solucions completes, CISCO, HP, i Aruba Networks, així mateix, en el sector LAN també és molt important l'empresa Juniper Networks que pot oferir solucions molt potents.

L'empresa es va posicionar a utilitzar elements de xarxa, com són switchs i routers, de la marca Cisco, principalment.

Font: Gartner, Fabricants sistemes LAN



Source: Gartner (January 2011) As of January 2011

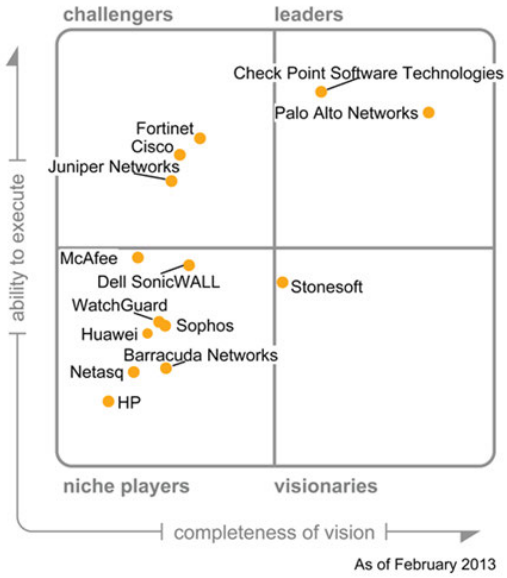
Com a fabricants de servidors, trobem en el mercat un conjunt de servidors molt ben posicionats en el mercat, entre els que destaquen HP, IBM i DELL. Tots tres ofereixen opcions de servidors molt competitius i molt interessants.

Podem trobar d'HP, solucions amb els models HP ProLiant, que és el que la nostre empresa va decidir instal·lar, concretament, el model: HP ProLiant ML350e Gen8.

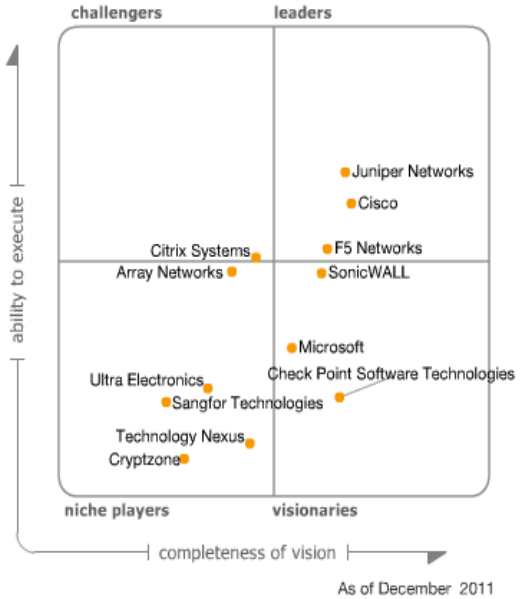
Font: Gartner, Fabricants sistemes servidors

Un altre aspecte molt important són els sistemes Firewall, en aquest quadre podem veure que algunes de les empreses més importants o més ben situades són Check Point Software, Palo Alto Networks, novament Cisco, i també Juniper Networks.

Totes aquestes empreses ofereixen sistemes molt potents, i sistemes integrats que ens permeten tenir una infraestructura segura en la nostre empresa. En aquest cas és va decidir per instal·lar els sistemes de Cisco.



Font: Gartner, Fabricants sistemes Firewall



En el que fa referència al cas de les SSL VPN, podem trobar empreses com Juniper Networks, Cisco, o F5 Networks, empreses molt importants en aquest sector. Cisco ens ofereix solucions punteres en el mercat de xarxes i seguretat, amb el programari Cisco IOS (AutoQoS, QoS Policy Manager, Intelligent Gateway Service, Solution Center IP...).

Font: Gartner, Fabricants sistemes SSL VPN

Pel que fa a Cisco, disposem dels Firewall ASA, que conté múltiples eines de seguretat, per exemple, el switch Cisco Catalyst 7000 Series que conté sistemes VPN, accés remot, firewall i inclús seguretat per IPS, d'última generació i que inclouen un rendiment i fiabilitat molt alta, així com serveixen per implementacions Cloud i virtualitzades, amb unes especificacions de 10, 40, i 100 Gigabits Ethernet.

En el cas de l'emmagatzematge s'utilitza un sistema NAS/SAN (Storage Area Network) pel centre de dades, que és una xarxa d'emmagatzematge de dades, i en que s'accedeix mitjançant programari, no com una xarxa apart, sinó que és com un disc dur connectat a grans velocitats, i molt útil en sistemes en que és gestionarà molta informació alhora.

La solució més adequada que es va trobar en aquell moment és de l'empresa DELL, amb els servidors rack PowerVault MD3620f, en el que podem guardar fins a 24 discs de 3,5" o 2,5" de 4tb cadascun, i utilitzant fins a 64 aplicacions diferents simultàniament, així mateix també existeixen models similars de la empresa HP.

Per evitar una possible pèrdua de dades, estan configurats els discs en mode RAID, així com també s'utilitza la tecnologia de que disposa Dell, la Dynamic Disk Pools (DDP), que millora la protecció de dades. Per gestionar els discs durs SAN o els servidors, s'utilitza una eina de Dell, integrada pel seu maquinari, anomenada OpenManage.

1.2.4. Autentificació i sistemes de seguretat del sistema, actual i futur:

Perquè el nostre sistema sigui el suficientment segur disposa d'un servei d'autentificació dels diferents usuaris del portal web, de l'aplicació mòbil i dels empleats de l'empresa, així com dels possibles programaris.

Un dels processos més importants en un sistema que conté informació confidencial, i amb un cert grau de seguretat és el de l'autentificació, per tant, cal que els usuaris que utilitzen el portal web tinguin el convenciment que la seva informació està segura, per conseqüent, augmenti la seva satisfacció amb el portal web.

Un dels sistemes més coneguts d'autentificació és la utilització de contrasenyes que els usuaris configuraren en el seu registre d'usuaris en el sistema. I que el sistema vetlla perquè aquesta contrasenya tingui un suficient grau de seguretat, com pot ser, un nombre mínim de caràcters, la utilització de caràcters alfanumèrics i l'ús de les majúscules i les minúscules en la mateixa clau d'accés.

Així mateix, cada empleat de l'empresa té assignat un nom d'usuari amb el que haurà d'accedir al seu equip, i mitjançant LDAP l'usuari podrà accedir a d'altres recursos i funcionalitats del sistema que siguin necessàries per la seva tasca diària. L'administració dels diferents recursos correspon al departament d'informàtica.

Pels empleats de l'empresa, és molt útil la utilització de targetes criptogràfiques d'autentificació, i targetes d'identitat, o que també podem anomenar targetes intel·ligents amb combinació d'una clau o PIN que només l'usuari coneix, que ens permetran controlar completament tothom que entra i surt de les diferents dependències sensibles, i per tant, verificar-ne la seva identitat en equips i sistemes. Per augmentar més la seguretat, fins i tot podríem implantar en un futur mètodes de verificació

biomètrica, com poden ser amb la verificació de veu, empremtes digitals, o amb mètodes oculars.

Els empleats de l'empresa abans de començar a treballar signa una política de confidencialitat, per evitar que pugui sortir informació de l'empresa. En el cas que s'utilitzen alguna empresa externa també s'aplicarien contractes per aquests treballs puntuals. Un cop una persona deixa l'empresa s'eliminen els seus permisos i es retornen a l'empresa els actius utilitzats.

De totes formes existeixen molts elements interns de la xarxa d'empleats, per exemple, que són millorables, com pot ser la freqüència obligatòria d'instal·lació d'actualitzacions en equips dels empleats, o un registre complet d'entrades i sortides d'equipament informàtic, per treballar fora de l'oficina, per exemple.

Per poder accedir a l'edifici de l'empresa es necessari passar per uns torns d'accés que només s'obren amb una targeta intel·ligent d'identitat de l'empleat, o mitjançant la targeta d'invitat que s'activa a recepció després de la comprovació del DNI, i l'autorització prèvia corresponent. Les dependències i l'exterior de l'empresa està controlat per un sistema de videovigilància i un vigilant de seguretat privada.

Pel que fa a la infraestructura, també s'ha tingut en compte de situar un servidor, que s'anomena de seguretat, i que està en la frontera de la xarxa amb internet per mitigar atacs de DoS, així com també compte amb un firewall, i un sistema de detecció de intrusions i prevenció per monitorar la xarxa.

També és útil per la infraestructura la DMZ, per poder aïllar els servidors exposats fora del centre de dades, de la resta de la xarxa. D'aquesta manera, podem assegurar que els atacs externs no afectaran els recursos interns del centre de dades.

Com a possible millora de futur per l'empresa, també podria ser important incloure en el sistema un sistema d'autentificació basat en la federació d'identitats o Single Sing-On, que ens permeti amb una sola instància de identificació poder autentificar-nos en múltiples sistemes diferents. N'existeixen diferents que és podrien utilitzar, com poden ser OpenID, Web-SSO, Kerberos, o Identitat federada.

Per tenir la suficient seguretat en la nostra informació i les dades empresarials, tant pròpies, com dels clients, també pot ser important utilitzar en un futur en alguns sistemes la combinació d'alguns d'algoritmes criptogràfics, de clau secreta (DES, AES, RC5), o de clau pública (Diffie-Hellman, RSA, DSA), o fins i tot algoritmes de hash (MD5, SHA), i amb combinació de diferents protocols segurs com poden ser, PGP, SSH, SSL, TLS, entre molts d'altres.

També pot ser important per a la nostre empresa disposar d'un anàlisi de riscs del sistema, amb identificació de les amenaces, riscos, i vulnerabilitats del nostre sistema, amb els corresponents plans de contingència, en el cas que sorgissin alguna incidència, ja que actualment no existeixen plans específics de documentació que detallin procediments de gestió d'incidents i de continuïtat del negoci

L'anàlisi detallat de les vulnerabilitats serà clau per tal de que tinguem identificats tots els possibles problemes del nostre sistema, ja que poden existir vulnerabilitats del propi

personal, relacionades amb amenaces estructurals, relacionades amb el hardware, amb les xarxes, amb la informació, o amb el software del nostre sistema. Per tant, un pla de seguretat que inclogui mesures preventives, mesures correctives i els riscos assumibles també pot ser molt útil en la nostre empresa.

La monitorització del sistema:

Un punt molt important del nostre sistema és la monitorització exhaustiva del mateix.
Cal tenir en compte, que l'aplicació del portal web, i l'aplicació mòbil estan funcionant les 24 hores del dia, i tots els dies de l'any, per tant, perquè això segueixi així cal portar a terme una monitorització contínua.

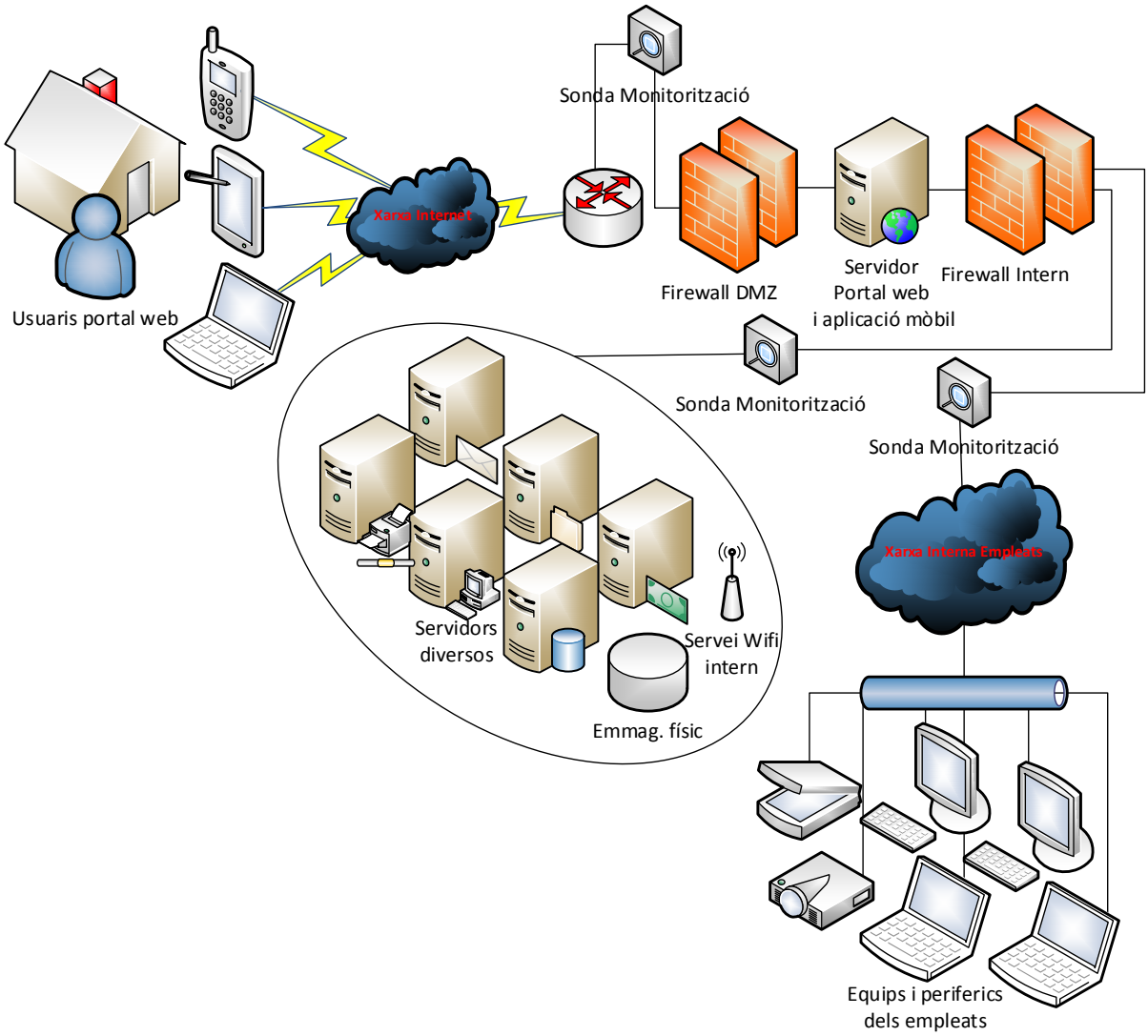
Aquesta monitorització es portada a terme per un conjunt de tests que es van executant periòdicament, i que avisen a l'administrador en cas que alguna cosa vagi malament. Fins i tot, podem simular carregues d'usuaris per saber si el sistema aguanta un pic d'usuaris en un moment donat. Podem monitoritzar, per exemple, les aplicacions, els serveis, els servidors, les comunicacions, els sistemes operatius d'aquests servidors, o les diferents bases de dades.

La nostra infraestructura de l'empresa, hauria de poder tenir més sistemes redundants, poder tenir una alta disponibilitat. Així mateix també hauria de poder disposar d'un anàlisi de riscos, una documentació de polítiques i normatives completa, consultable i revisable, i un pla de continuïtat del negoci, per si sorgeix algun imprevist o alguna incidència que haurem de solucionar en el mínim possible. Així mateix també podríem dotar el sistema de serveis duplicats, que puguin començar a funcionar automàticament en cas de fallada, i d'aquesta forma els diferents serveis queden afectats al mínim.

Un bon programari lliure que utilitzen moltes empreses i organitzacions per dur a terme aquesta monitorització és el sistema Nagios, que ofereix grans funcionalitats de monitorització. Podem trobar més informació en l'enllaç http://www.nagios.com. Així mateix podem visualitzar diferents captures de pantalla de les diferents funcionalitats possibles en el següent enllaç http://www.nagios.com/products/nagioscore/screenshots.

1.2.5. Esquema de la infraestructura de l'empresa:

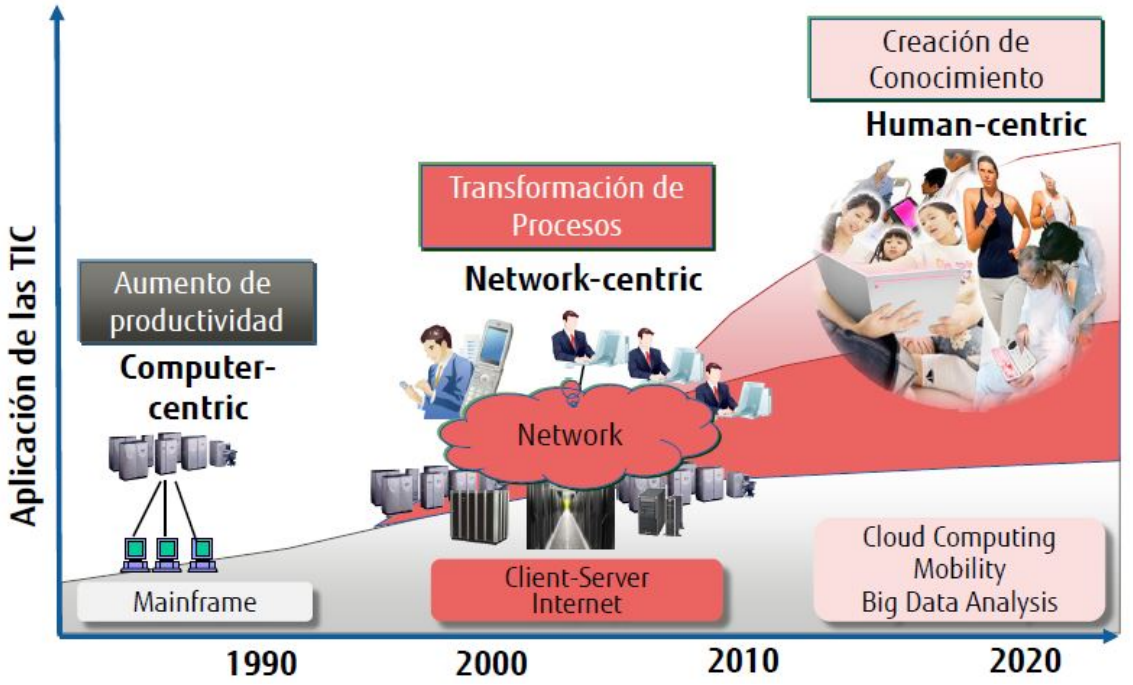
La infraestructura de l'empresa la podem resumir amb el següent diagrama, que ens informa de manera genèrica dels principals elements de que disposa l'empresa (no és un diagrama de la infraestructura detallat, sinó que l'objectiu és que serveixi de introducció a la infraestructura de l'empresa de forma genèrica).



1.2.5. L'augment de dades a tractar a la nostre l'empresa – El Big-Data:

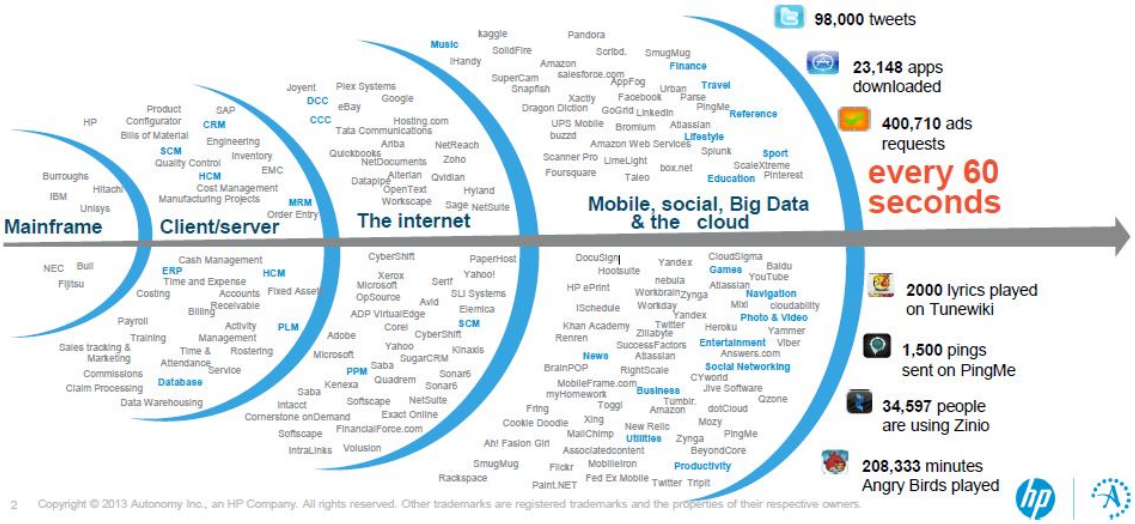
En les següents línies faré una mica de ressenya a com han evolucionat i augmentat les dades a que hauran de fer front les empreses que tinguin una infraestructura web i que tinguin que tractar dades de xarxes socials, per màrqueting, o per les seves pròpies tasques diàries.

En la següent imatge podem veure l'evolució des dels anys 90, amb els sistemes mainframe, passant pels anys 2000-2008 amb els sistemes client i servidor, i arribant als dies actuals en que és fa necessari l'anàlisi i tractament de grans quantitats de dades, l'anomenat Big-Data.



Font de dades: Presentació Big Data de Fujitsu 2013

L'augment de dades ha estat produït per l'increment d'utilització massiva d'Internet per part de perfils d'usuaris, com són els usuaris particulars, les grans multinacionals, les organitzacions, les empreses, els governs, amb l'administració electrònica, i la gran facilitat de la generació actual d'usuaris, de poder enviar missatges, correus, comentaris a xarxes socials, la utilització de les eines dels telèfons mòbils, o qualsevol altre aplicació que generi dades i les permeti compartir a través de la xarxa Internet.

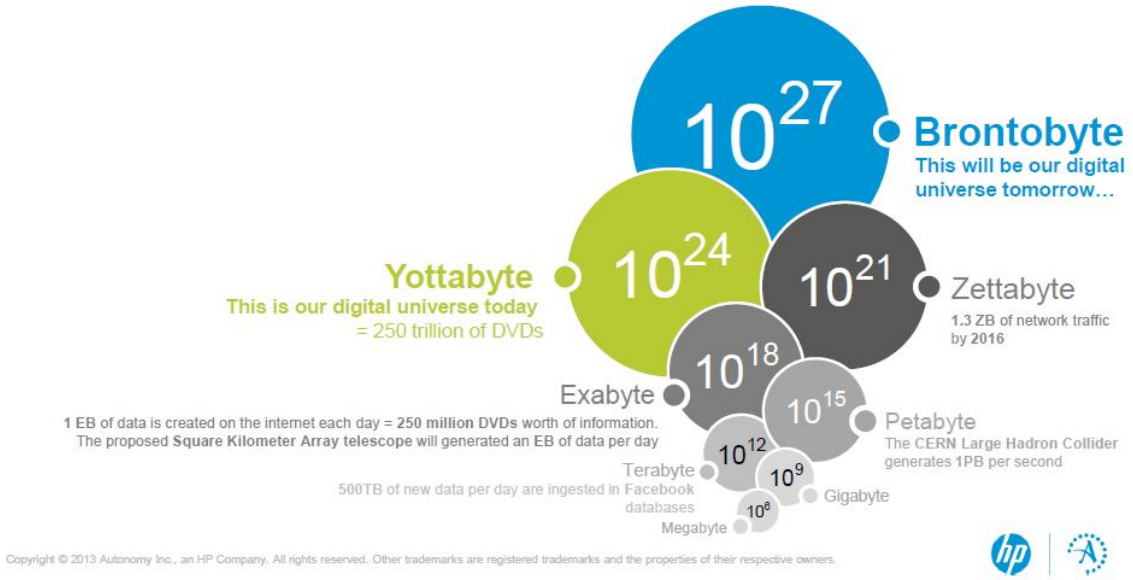


Font de dades: Presentació Big-Data de Hewlett-Packard 2013

Com podem veure en la imatge anterior, el Big-Data, suposa per la generació actual, i per les infraestructures tecnològiques i de seguretat actual, un gran repte al que s'han d'enfrontar per poder seguir liderant el mercat i poder aconseguir el avantatge competitiu que qualsevol organització desitja disposar.

Així mateix, l'augment de dades, fa que els actuals sistemes d'emmagatzematge i els servidors actuals hagin d'estar preparats per suportar una gran immensitat de dades, i

que tot seguit podem veure en el diagrama, alguns dels nous termes que les organitzacions i les empreses de serveis d'Internet han de començar a adoptar per mantenir-se líders del mercat.



Font de dades: Presentació Big Data de Hewlett-Packard 2013

Per tant, com hem vist, el Big-Data suposa un gran repte al que hem de fer front si volem poder analitzar i tractar les valuoses dades dels potencials clients.

En aquest projecte, per tant, haurem de tenir en compte que un augment exponencial de les dades a tractar i per tant una infraestructura molt més gran sempre necessitarà una major seguretat de les dades a tractar, i això també s'haurà de tenir en compte a l'hora de fer front a les possibles noves amenaces i els objectius del pla director de seguretat.

1.3.Definició dels objectius del Pla Director de Seguretat:

Un punt molt important en qualsevol projecte que desitgi crear un pla director de seguretat per una organització o una empresa és tenir molt clars i ben definits els objectius que vol assolir aquest pla.
En aquesta primera fase del projecte s'inclouran els objectius més genèrics que podem pensar que són els més bàsics i alhora importants. A mesura que el projecte vagi agafant forma i contingut aquests objectius també poden créixer i especialitzar-se, tenint en compte el concepte de millora continua que sempre hem de tenir en compte i com a punt primordial.

Alguns objectius els podem veure en els següents punts:

- Hem de poder identificar el nivell de seguretat que disposa la nostre empresa en els seus sistemes, serveis, aplicacions i en la pròpia infraestructura de sistemes d'informació de l'empresa.

- Poder assegurar la integritat, disponibilitat i confidencialitat de la informació de la pròpia empresa, i dels clients de la mateixa.

- Hem de poder planificar projectes a realitzar a curt, mitjà i llarg termini, segons els problemes detectats en punts anteriors.

- Hem de poder preveure l'augment de la infraestructura i de les dades a tractar en un futur, ja que això afectaria a les mesures de seguretat actualment implantades.

- També haurem de tenir en compte que cadascun dels projectes té un cost, per tant s'hauran de prioritzar segons la necessitat que té l'empresa de disposar de les millores que proposa el projecte concret.

- Hem de poder crear directrius de seguretat pels diferents departaments, treballadors i infraestructures tecnològiques de l'empresa.

- Hem de poder realitzar un seguiment, i un sistema de millora continua de les diferents tasques que implantem per millorar la seguretat.

1.4.Anàlisis diferencial de l'empresa respecte a la ISO/IEC 27001+ISO/IEC 27002:

En aquest punt es realitzarà un anàlisi diferencial de les diferents mesures de seguretat i la normativa de que disposa la nostre empresa, amb relació a la seguretat de la informació, permetent-nos tenir una primera idea de l'estat actual respecte la ISO/IEC 27001 i la ISO/IEC 27002.

Cal dir també que la ISO/IEC 27002, prové de l'anterior ISO 17799, on podem trobar un conjunt de controls, que marquen les bases per tenir un manual de "bones pràctiques" que les organitzacions poden adoptar i utilitzar amb els seus sistemes de seguretat.

Tot seguit podem veure el quadre d'anàlisis diferencial:

ANÀLISIS DIFERENCIAL ISO 27001 - 27002		
TIPUS DE CONTROL ISO	**COMPLEIX?**	**OBSERVACIONS**
5. Política de seguretat		
5.1. Política de seguretat de la informació		
5.1.1. Document de política de seguretat de la informació	**NO COMPLEIX**	L'empresa disposa del document però no s'actualitza ni revisa.
5.1.2. Revisió de la política de seguretat de la informació	**NO COMPLEIX**	Es necessita una actualització i revisió de la política de seguretat.
6. Aspectes organitzatius de la seguretat de la informació		
6.1. Organització interna		
6.1.1. Compromís de la direcció amb la seguretat de la informació	**COMPLEIX**	La direcció està convençuda i compromesa amb la seguretat, vol disposar de totes les mesures necessàries, tenint sempre en compte la relació cost/eficàcia
6.1.2. Coordinació de la seguretat de la informació	**COMPLEIX**	El departament de IT és el responsable de la coordinació en temes de seguretat.
6.1.3. Assignació de	**COMPLEIX**	El departament de IT és

responsabilitats relatives a la seguretat de la informació		l'encarregat de les tasques de seguretat.
6.1.4. Procés d'actualització de recursos pel tractament de la informació	**NO COMPLEIX**	No està correctament especificats els rols de seguretat.
6.1.5. Acords de confidencialitat	**COMPLEIX**	Existeixen acords de confidencialitat pels treballadors de l'empresa
6.1.6. Contacte amb les autoritats	**NO COMPLEIX**	En el cas que hi hagués algun problema que requerís el contacte amb autoritats és realitzaria, però no està especificat.
6.1.7. Contacte amb grups d'especial interès	**NO COMPLEIX**	No s'ha especificat cap contacte amb grups d'especial interès.
6.1.8. Revisió independent de la seguretat de la informació	**NO COMPLEIX**	No s'ha tingut en compte que és realitzi una revisió independent de la seguretat de la informació.
6.2. Tercers		
6.2.1. Identificació dels riscos derivats de l'accés de tercers	**NO COMPLEIX**	No estan especificats els riscos d'accés de tercers.
6.2.2. Tractament de la seguretat en la relació amb els clients	**COMPLEIX**	S'apliquen diferents nivells de seguretat segons les dades de que es disposen dels clients.
6.2.3. Tractament de la seguretat en contractes amb tercers	**NO COMPLEIX**	No s'ha especificat.
7. Gestió d'actius		
7.1. Responsabilitat sobre els actius		
7.1.1. Inventari d'actius	**NO COMPLEIX**	Es disposa d'un inventari d'actius, però no està actualitzat ni revisat.
7.1.2. Propietat dels actius	**COMPLEIX**	S'especifica en l'inventari la propietat de cada actiu.
7.1.3. Ús acceptable dels actius	**COMPLEIX**	Existeix una política que els usuaris han d'acceptar i respectar.
7.2. Classificació de la informació		
7.2.1. Directrius de classificació	**COMPLEIX**	Es classifica la informació segons la seva sensibilitat o segons el seu nivell crític.
7.2.2. Etiquetat i manipulat de la informació	**COMPLEIX**	S'utilitza un gestor documental per la documentació de que disposa l'empresa.
8.Seguretat lligada als recursos humans		
8.1. Abans de la feina		
8.1.1. Funcions i responsabilitats	**COMPLEIX**	Es contracta als treballadors segons els seus rols o perfils de funcions.
8.1.2. Investigació d'antecedents	**COMPLEIX**	El departament de RRHH s'encarrega de la tasca.
8.1.3. Termes i condicions de contractació	**COMPLEIX**	En el moment de la contractació els empleats firmen les condicions i la confidencialitat.

8.2. Durant la feina		
8.2.1. Responsabilitats de la direcció	**COMPLEIX**	S'apliquen uns rols de responsabilitat determinats.
8.2.2. Conscienciació, formació i capacitació en seguretat de la informació	**COMPLEIX**	L'empresa dedica alguna part del pressupost a la formació en seguretat pels seus empleats.
8.2.3. Procés disciplinari	**NO COMPLEIX**	Es pressuposa que existeix, però no se'n coneix el contingut escrit.
8.3. Finalització de la feina o canvi de lloc de treball		
8.3.1. Responsabilitat de finalització o canvi	**COMPLEIX**	S'apliquen els rols de responsabilitat determinats.
8.3.2. Devolució d'actius	**COMPLEIX**	Un cop finalitzat, s'han de realitzar la devolució d'actius que han sigut entregats a l'empleat.
8.3.3. Retirada de drets d'accés	**COMPLEIX**	El departament de IT retira els drets d'accessos al sistema de l'empleat donat de baixa.
9. Seguretat física i de l'entorn		
9.1. Àrees segures		
9.1.1. Perímetre de seguretat física	**COMPLEIX**	Existeixen diferents mesures de seguretat exterior, com poden ser càmeres, sensors i vigilants.
9.1.2. Controls físics d'entrada	**COMPLEIX**	El control físic d'entrada es realitza mitjançant una targeta unipersonal.
9.1.3. Seguretat d'oficines, despatxos i instal·lacions	**COMPLEIX**	Les dependències amb material sensible, com servidors, està controlat per codis PIN, i sensors de moviment.
9.1.4. Protecció contra les amenaces externes i d'origen ambiental	**NO COMPLEIX**	El subministrament elèctric disposa de SAI's de suport, però són insuficients.
9.1.5. Treball en àrees segures	**NO COMPLEIX**	No es pot assegurar que siguin àrees segures, ja que podrien accedir-hi altres persones, amb el mateix codi PIN.
9.1.6. Àrees d'accés públic i de càrrega i descarrega	**NO COMPLEIX**	No existeix una àrea especifica de càrrega i descarrega.
9.2. Seguretat dels equips		
9.2.1. Distribució i protecció dels equips	**NO COMPLEIX**	Algunes dependències disposen d'accés amb PIN, els despatxos normals no.
9.2.2. Instal·lacions de subministrament	**NO COMPLEIX**	El subministrament elèctric disposa de SAI's de suport.
9.2.3. Seguretat del cablejat	**NO COMPLEIX**	No s'ha especificat.
9.2.4. Manteniment dels equips	**NO COMPLEIX**	El manteniment el realitza el departament de IT, però s'hauria de millorar.
9.2.5. Seguretat dels equips de	**NO**	No existeix una seguretat dels

fora les instal·lacions	**COMPLEIX**	equips que surten de les instal·lacions, excepte per l'ús de VPN's.
9.2.6. Reutilització o retirada segura d'equips	**NO COMPLEIX**	Un cop es retiren els equips es dipositen a empreses residus, però no es realitza un format a baix nivell, només un de normal.
9.2.7. Retirada de materials propietat de l'empresa	**COMPLEIX**	Es necessita omplir un imprès i aquest ha de ser autoritzat.
10. Gestió de comunicacions i operacions		
10.1.Responsabilitats i procediments d'operació		
10.1.1. Documentació dels procediments d'operació	**NO COMPLEIX**	No estan completament documentats.
10.1.2. Gestió de canvis	**COMPLEIX**	Els canvis són duts a terme de manera definida.
10.1.3. Segregació de tasques	**COMPLEIX**	Es segreguen tasques segons els especialistes.
10.1.4. Separació dels recursos de desenvolupament, prova i operació	**COMPLEIX**	Es compleix aquesta separació de recursos segons la seva tipologia.
10.2. Gestió de la provisió de serveis per tercers		
10.2.1. Provisió de serveis	**NO COMPLEIX**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.2.2. Supervisió i revisió dels serveis oferts per tercers	**NO COMPLEIX**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.2.3. Gestió del canvi en els serveis oferts per tercers	**NO COMPLEIX**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.3. Planificació i acceptació del sistema		
10.3.1. Gestió de capacitats	**COMPLEIX**	S'avalua la capacitat de la infraestructura periòdicament.
10.3.2. Acceptació del sistema	**COMPLEIX**	Es realitza la acceptació quan es comprova que tot funciona correctament.
10.4. Protecció contra el codi maligne i descarregues		
10.4.1. Controls contra el codi maligne	**COMPLEIX**	Es disposa de programari de detecció de virus i programaris malignes que s'actualitza diàriament.
10.4.2. Controls contra el codi descarregat en el client	**COMPLEIX**	Es disposa d'unes normes que prohibeixen el codi descarregat de tercers en l'empresa si no se sap l'origen confiable.
10.5. Copies de seguretat		
10.5.1. Copies de seguretat de la informació	**NO COMPLEIX**	Es realitza periòdicament un backup de dades dels servidors i dels discs durs del sistema, però no

		de les dades locals dels equips personals dels treballadors.
10.6. Gestió de la seguretat de les xarxes		
10.6.1. Controls de xarxa	**COMPLEIX**	La xarxa es controlada per programaris de monitoreig, tipus Nagios, i programaris de firewall.
10.6.2. Seguretat dels serveis de xarxa	**COMPLEIX**	Els programaris de seguretat controles els diferents serveis de la xarxa, per assegurar-ne el correcte funcionament.
10.7. Manipulació dels suports		
10.7.1. Gestió de suports extraïbles	**NO COMPLEIX**	No existeix actualment.
10.7.2. Retirada de suports	**NO COMPLEIX**	Si són suports de disc durs és realitza un format, però no de baix nivell.
10.7.3. Procediments de manipulació de la informació	**COMPLEIX**	La informació es classifica i es manipula segons si es critica i segons els rols dels treballadors.
10.7.4. Seguretat de la documentació del sistema	**COMPLEIX**	La documentació dels sistema en té accés els perfils adequats, del gestor documental.
10.8. Intercanvi de informació		
10.8.1. Polítiques i procediments de intercanvi de informació	**NO COMPLEIX**	No està especificat.
10.8.2. Acords de intercanvi	**NO COMPLEIX**	No estan especificats.
10.8.3. Suports físics en transit	**NO COMPLEIX**	No està especificat.
10.8.4. Missatgeria electrònica	**COMPLEIX**	S'utilitza per tasques internes de treballadors de la pròpia empresa.
10.8.5. Sistemes de informació empresarial	**COMPLEIX**	Es disposa d'un sistema de informació empresarial amb gestor documental.
10.9. Serveis de comerç electrònic		
10.9.1. Comerç electrònic	**COMPLEIX**	El comerç electrònic del portal web està especificat.
10.9.2. Transaccions en línia	**COMPLEIX**	S'utilitza un sistema de transaccions en línia segures.
10.9.3. Informació públicament disponible	**COMPLEIX**	S'utilitzen sistemes de seguretat per evitar intrusions.
10.10. Supervisió		
10.10.1. Registres d'auditoria	**NO COMPLEIX**	No s'han realitzat auditories, però el sistema disposa d'un sistema de logs.
10.10.2. Supervisió de l'ús del sistema	**COMPLEIX**	El propi sistema monitoritza l'ús del sistema, per detectar comportaments inadequats

10.10.3. Protecció de la informació dels registres	**COMPLEIX**	Els logs estan protegits per les pròpies eines del sistema.
10.10.4. Registres d'administració i operació	**COMPLEIX**	Els registres queden guardats al servidor.
10.10.5. Registre de fallades	**COMPLEIX**	Les incidències queden registrades, i posteriorment a la solució, es documenten i arxiven.
10.10.6. Sincronització de rellotge	**COMPLEIX**	El servidor disposa de la sincronització de rellotge.
11. Control d'accés		
11.1. Requisits de negoci pel control d'accés		
11.1.1. Política de control d'accés	**COMPLEIX**	L'accés es realitza mitjançant una política de control d'accés a les instal·lacions critiques.
11.2. Gestió d'accés d'usuari		
11.2.1. Registre d'usuari	**COMPLEIX**	Existeix un procediment de registre d'usuaris.
11.2.2. Gestió de privilegis	**COMPLEIX**	Existeix una gestió dels privilegis dels diferents tipus o perfils d'usuaris.
11.2.3. Gestió de contrasenyes d'usuari	**COMPLEIX**	Existeix una gestió de les contrasenyes dels diferents perfils d'usuaris.
11.2.4. Revisió dels drets d'accés d'usuari	**COMPLEIX**	Es revisen els drets d'accés dels usuaris segons els seus perfils o canvis de perfils.
11.3. Responsabilitats d'usuari		
11.3.1. Ús de contrasenyes	**COMPLEIX**	Existeix una política d'ús i creació de contrasenyes.
11.3.2. Equip d'usuari desatès	**NO COMPLEIX**	Existeix una normativa antiga, però necessita una revisió i recordar-la als usuaris.
11.3.3. Política de lloc de treball buit i pantalla neta	**NO COMPLEIX**	Existeix una normativa antiga, però necessita una revisió i recordar-la als usuaris.
11.4. Control d'accés a xarxa		
11.4.1. Política d'ús dels serveis de xarxa	**NO COMPLEIX**	Existeix una política d'ús dels serveis de xarxa, però necessita una revisió.
11.4.2. Autentificació d'usuari per connexions externes	**COMPLEIX**	Es disposa d'accés per VPN.
11.4.3. Identificació dels equips en les xarxes	**COMPLEIX**	Els equips queden registrats i identificats en les xarxes en les que es connecten.
11.4.4. Diagnòstic remot i protecció dels ports de configuració	**COMPLEIX**	Les eines del sistema permeten un diagnòstic remot i protecció de ports.
11.4.5. Segregació de les xarxes	**COMPLEIX**	Existeixen diferents xarxes segregades segons funcions.

11.4.6. Control de la connexió a la xarxa	**COMPLEIX**	Les connexions a la xarxa estan controlades per programari del sistema.
11.4.7. Control d'encaminament (Routing) de xarxa	**COMPLEIX**	El tràfic passa per firewalls i protocols que controlen la xarxa.
11.5. Control d'accés al sistema operatiu		
11.5.1. Procediments segurs d'inici de sessió	**COMPLEIX**	Es disposa de noms d'usuari, contrasenyes, i certificats a disposició dels diferents perfils d'usuaris.
11.5.2. Identificació i autentificació d'usuari	**COMPLEIX**	Es realitza una identificació i autentificació dels diferents perfils d'usuaris.
11.5.3. Sistema de gestió de contrasenyes	**COMPLEIX**	Es realitza una gestió de les diferents contrasenyes dels sistemes.
11.5.4. Ús dels recursos del sistema	**COMPLEIX**	Es controla mitjançant programari l'ús dels diferents recursos del sistema.
11.5.5. Desconnexió automàtica de sessió	**COMPLEIX**	Al cap d'un temps determinat d'inactivitat es desconnecta la sessió.
11.5.6. Limitació de temps de connexió	**NO COMPLEIX**	No existeix actualment.
11.6. Control d'accés a les aplicacions i a la informació		
11.6.1. Restricció de l'accés a la informació	**NO COMPLEIX**	Es pot restringir l'accés a la informació de que disposen els servidors, però la informació en equips personals no sempre es tan segura.
11.6.2. Aïllament de sistemes sensibles	**COMPLEIX**	Els sistemes més sensibles estan aïllats de la resta de la xarxa.
11.7. Ordinadors portàtils i teletreball		
11.7.1. Ordinadors portàtils i comunicacions mòbils	**NO COMPLEIX**	No existeix un control eficaç de les comunicacions mòbils i portàtils.
11.7.2. Teletreball	**COMPLEIX**	Es pot realitzar mitjançant una VPN.
12. Adquisició, desenvolupament i manteniment dels sistemes de informació		
12.1. Requisits de seguretat dels sistemes de informació		
12.1.1. Anàlisi i especificació dels requisits de seguretat	**COMPLEIX**	Es comproven que en els canvis i nous desenvolupaments es segueixin els requisits de seguretat necessaris en cada cas.
12.2. Tractament correcte de les aplicacions		
12.2.1. Validació de les dades d'entrada	**COMPLEIX**	El programari valida que les dades d'entrada siguin correctes.
12.2.2. Control de processament intern	**COMPLEIX**	El programari valida el processament intern.
12.2.3. Integritat dels missatges	**COMPLEIX**	S'assegura la integritat dels

		missatges que el programari envia.
12.2.4. Validació de les dades de sortida	**COMPLEIX**	El programari valida les dades de sortida.
12.3. Controls criptogràfics		
12.3.1. Política d'ús dels controls criptogràfics	**NO COMPLEIX**	No s'especifica documentalment.
12.3.2. Gestió de claus	**NO COMPLEIX**	No s'especifica documentalment.
12.4. Seguretat dels arxius del sistema		
12.4.1. Control del programari en explotació	**NO COMPLEIX**	Existeixen procediments que han de ser revisats.
12.4.2. Protecció de les dades de prova del sistema	**NO COMPLEIX**	Existeixen procediments que han de ser revisats.
12.4.3. Control d'accés al codi font dels programes	**COMPLEIX**	El accés al codi font dels programes està protegit.
12.5. Seguretat en el procés de desenvolupament i suport		
12.5.1. Procediments de control de canvis	**COMPLEIX**	Es realitzen procediments de control de canvis.
12.5.2. Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	**COMPLEIX**	Es comprova el bon funcionament després d'efectuar canvis en el sistema operatiu.
12.5.3. Restriccions als canvis en els paquets de programari	**NO COMPLEIX**	No existeixen restriccions concretes als canvis en els paquets de programari.
12.5.4. Fugues de informació	**NO COMPLEIX**	No existeix cap control específic, però el contracte de confidencialitat ho prohibeix.
12.5.5. Externalització del desenvolupament de programari	**NO COMPLEIX**	No s'externalitza el desenvolupament de programari.
12.6. Gestió de la vulnerabilitat tècnica		
12.6.1. Control de les vulnerabilitats tècniques	**NO COMPLEIX**	Existeix un registre de vulnerabilitats detectades, que hauria de ser revisat.
13. Gestió de incidents de seguretat de la informació		
13.1. Notificació d'esdeveniments i punts dèbils de seguretat de la informació		
13.1.1. Notificació d'esdeveniments de seguretat de la informació	**COMPLEIX**	Es registren els esdeveniments i es documenten les solucions.
13.1.2. Notificació de punts dèbils de seguretat	**COMPLEIX**	Es documenten i s'intenten millorar o reforçar els punts dèbils del sistema.
13.2. Gestió de incidents de seguretat de la informació i millores		
13.2.1. Responsabilitats i procediments	**COMPLEIX**	Existeix un document que especifica les responsabilitats.
13.2.2. Aprenentatge dels incidents de seguretat de la informació	**COMPLEIX**	Els incidents després de ser solucionats es documenten per futures consultes.
13.2.3. Recopilació d'evidències	**COMPLEIX**	Les evidències es documenten i s'arxiven.

14. Gestió de la continuïtat del negoci		
14.1. Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci		
14.1.1. Inclusió de la seguretat de la informació en el procés de gestió de la continuïtat del negoci	**NO COMPLEIX**	No s'ha especificat un pla de continuïtat del negoci.
14.1.2. Continuïtat del negoci i avaluació de riscs	**NO COMPLEIX**	No s'ha especificat un pla de continuïtat del negoci.
14.1.3. Desenvolupament i implantació de plans de continuïtat que incloguin la seguretat de la informació	**NO COMPLEIX**	No s'ha especificat un pla de continuïtat del negoci.
14.1.4. Marc de referència per la planificació de la continuïtat del negoci	**NO COMPLEIX**	No s'ha especificat un pla de continuïtat del negoci.
14.1.5. Proves, manteniment i re-avaluació dels plans de continuïtat del negoci	**NO COMPLEIX**	No s'ha especificat un pla de continuïtat del negoci.
15. Compliment		
15.1. Compliment dels requisits legals		
15.1.1. Identificació de la legislació aplicable	**COMPLEIX**	La legislació aplicable esta documentada i es té en compte.
15.1.2. Drets de propietat intel·lectual (IPR)	**COMPLEIX**	Els drets de propietat intel·lectual estan perfectament definits.
15.1.3. Protecció dels documents de l'organització	**COMPLEIX**	Els documents de l'empresa estan protegits legalment.
15.1.4. Protecció de dades i privacitat de la informació de caràcter personal	**COMPLEIX**	L'empresa té un seguiment de la LOPDP, en el que fa referència a les dades de caràcter personal.
15.1.5. Prevenció d'ús indegut dels recursos de tractament de la informació	**COMPLEIX**	El marc legal de l'empresa indica les conseqüències de l'ús indegut dels recursos.
15.1.6. Regulació dels controls criptogràfics	**NO COMPLEIX**	No està especificat.
15.2. Compliment de les polítiques i normes de seguretat i compliment tècnic		
15.2.1. Compliment de les polítiques i normes de seguretat	**NO COMPLEIX**	En l'actualitat encara no s'ha realitzat una auditoria que ens permeti saber el compliment de les polítiques i normes de seguretat.
15.2.2. Comprovació del compliment tècnic	**NO COMPLEIX**	No s'ha realitzat una comprovació del compliment tècnic.
15.3. Consideracions sobre la auditoria dels sistemes de informació		
15.3.1. Controls d'auditoria dels sistemes de informació	**NO COMPLEIX**	No s'ha realitzat fins a l'actualitat controls d'auditoria dels sistemes d'informació.
15.3.2. Protecció de les eines d'auditoria dels sistemes de informació	**NO COMPLEIX**	No s'ha especificat la protecció de les eines d'auditoria dels sistemes d'informació.

1.5.Resultats de la primera fase:

Com hem pogut observar en els anteriors punts, en la empresa en qüestió hi ha la possibilitat de realitzar molts projectes que puguin ajudar a la millora de la seguretat dels diferents àmbits analitzats, i que s'analitzaran i especificaran en les següents fases del projecte.

Evidentment, l'empresa disposa de certs elements de seguretat que si que té controlats, de totes formes, existeixen molts altres elements que necessiten adaptar-se als estàndards i augmentar la seguretat per evitar pèrdues d'informació, i per aconseguir que puguem assegurar que la informació d'aquesta empresa està sempre disponible, té integritat, i té la confidencialitat necessària en cada cas.

Per resumir-ho en un punts podem dir:

- L'abast del projecte s'ha centrat en els sistemes d'informació de l'empresa, i els elements organitzatius relacionats.
- Falta de seguretat en molts aspectes, des de la formació dels empleats, fins a la seguretat dels propis equipaments auxiliars, documentacions, maquinari, aplicacions i xarxes utilitzades.
- Falta d'una documentació actualitzada, i revisada.
- Falta assegurar en molts aspectes les dimensions de seguretat:
    - Autenticitat
    - Confidencialitat
    - Integritat
    - Disponibilitat
    - Traçabilitat
- Falta de rols propis en els treballadors de seguretat de la informació.

2. FASE II – Sistema de Gestió Documental:

En aquesta segona fase es farà incidència en el conjunt de documentació que ha de disposar el nostre sistema d'informació, i que venen establerts en la pròpia normativa ISO/EIC 27001. Tot seguit podem veure un resum de que hauria d'incloure bàsicament cada documentació.

2.1. Política de seguretat:

Encapçalament del document:

Codi	Politica_Seguretat_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Baixa

Historial de revisions:

Data	Versió	Autor	Descripció
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de la política de seguretat.
	....		
	....		

2.1.1. Introducció a la política de seguretat:

En aquesta documentació s'especificarà la normativa interna que pot tenir l'organització, i que els diferents perfils de treballadors de l'organització han de conèixer i complir degudament. S'especificaran temes relatius a l'accés a la informació, als recursos, o com actuar davant incidents.

La política de seguretat contemplarà l'ús adequat de tots els recursos tecnològics, per parts dels diferents perfils d'usuaris, amb la suficient confidencialitat, integritat, disponibilitat i autenticitat. Aquesta política haurà de ser actualitzada i revisada periòdicament, incloent els diferents canvis tecnològics que amb el temps incorpori el sistema d'informació de l'organització.

2.1.2. Objectius, missió i abast de la política de seguretat, i entrada en vigor:

El principal objectiu de la política de seguretat és tenir un marc normatiu que tothom de l'empresa pugui seguir, mitjançant unes bases que siguin seguides per tots els treballadors de l'empresa i personal vinculat a l'empresa.

Aquestes bases tracten de poder mantenir segurs els sistemes de seguretat de l'empresa, intentant minimitzar els riscos, i podent tenir un seguiment de la legislació vigent en

matèria de dades personals en els sistemes d'informació, i per tant, assegurant una disponibilitat, confidencialitat i integritat de totes les dades i sistemes de l'empresa.

La política haurà de ser posada en funcionament tant bon punt sigui acceptada pels responsables de l'empresa, i se'n hagi realitzat la suficient divulgació i formació per tots els empleats i personal vinculat a l'organització.

2.1.3. Procediment de la política general de l'organització:

L'organització estableix un conjunt de normatives generals per a tota l'empresa, que seran revisades pel comitè de seguretat de l'empresa, que alhora també s'encarregarà del seu compliment, i millora contínua.

- L'empresa implementarà els controls d'acord amb les normatives ISO que ha de seguir, i que li permetrà protegir la informació de l'empresa convenientment.

- Els actius de l'empresa seran degudament inventariats i classificats per poder ser protegits amb les mesures de seguretat necessàries en cada cas.

- Es protegirà la informació i canals de comunicació de la possible informació que l'empresa pugui compartir en el present o futur amb proveïdors, clients, i amb els diferents perfils d'empleats de l'empresa.

- Es fomentarà l'ús adequat segons la legislació vigent de les diferents tasques de l'empresa.

- L'empresa obliga a que tots els perfils d'usuari que utilitzin o manipulin algun tipus d'informació, aquesta ha de ser degudament protegida, i amb còpia de seguretat de les dades que estiguin en els propis equips.

- L'empresa obliga en l'ús de les seves tasques, a que els usuaris utilitzin únicament els equips i programaris degudament autoritzats per l'empresa, per evitar amenaces i riscos no controlats.

- El comitè de seguretat realitzarà controls i revisions periòdiques del sistema amb planificació i divulgació necessàries perquè tots els usuaris implicats en tinguin el màxim coneixement en el moment de produir-se.

- És obligatori que els diferents perfils d'usuaris informin de possibles errors, fallades de seguretat o incidents diversos, en els sistemes o programaris, i que puguin produir alguna pèrdua, o manipulació indeguda de les dades o del propi sistema.

- El responsable de seguretat disposarà d'un sistema de visualització d'incidències que es produeixin i que hagin sigut indicades pels mitjans establerts pel contacte (formulari d'incidències).

- Els responsables de seguretat realitzaran les tasques necessàries de difusió de la documentació de seguretat que permeti el correcte seguiment de les diferents polítiques de seguretat.

2.1.4. Gestió d'actius de l'organització:

- Tots els actius de l'organització hauran de ser degudament inventariats i assignats a un treballador, responsable del seu bon ús per les tasques que té encomanades dins de l'organització.

- Els actius seran degudament classificats segons la seva importància pel funcionament del sistema, i segons aquesta classificació se l'hi assignarà un nivell de seguretat i unes mesures especifiques, per protegir la integritat del sistema en cas de fallada.

- Els treballadors de l'empresa seran els encarregats de notificar qualsevol fallada o mal funcionament de l'actiu en el moment en que sigui detectat l'error, i aquests seran posats a disposició del departament corresponent sense demora, perquè puguin solucionar la incidència en el menor temps possible.

2.1.5. Gestió de recursos humans i organització:

- La coordinació de la seguretat dels sistemes de l'organització serà controlada pel departament de sistemes i pel comitè de seguretat.

- El comitè de seguretat definirà i assignarà les responsabilitats relatives a la seguretat de la informació de l'organització.

- Els treballadors que s'incorporin a l'organització, hauran de lliurar el seu CV a recursos humans, així com qualsevol documentació de feines anteriors o certificats d'antecedents, que recursos humans sol·liciti pel desenvolupament del procés de contractació.

- L'equip de treball del treballador i l'entorn de treball ha de ser net de notes i altres informacions que puguin ser sensibles o importants. Així mateix cal tenir la precaució de no deixar la sessió oberta mentre l'equip està desatès.

- Existeixen acords de confidencialitat que tot treballador o empresa que interactuï amb la nostra haurà d'acceptar i firmar.

- Qualsevol irregularitat manifesta d'algun acord, norma, o política de l'empresa, quedarà registrada i serà sancionada severament a criteri del departament de recursos humans de l'empresa, i el comitè de seguretat.

- Els casos més greus o que puguin implicar la comissió d'algun delicte, i sempre amb la presumpció d'innocència, seran immediatament comunicats a les diferents autoritats competents, ja siguin cossos de policia o diferents òrgans judicials o governamentals.

2.1.6. La seguretat física i el control d'accés:

- Els diferents actius estaran protegits, i segons la seva importància per l'organització, disposaran de sensors per controlar el seu bon funcionament, com

poden ser sensors d'humitat, sensors de temperatura, de subministrament elèctric, de moviment, així com equips de videovigilància.

- El control d'accés a l'edifici disposarà de diferents etapes segons la importància de la zona a protegir, per tant, podem trobar, tant controls personals d'accés, com accés a zones restringides protegides per claus / PIN's, i targetes intel·ligents, així com també es pot acordar implantar algun control biomètric en zones crítiques.

- Els diferents accessos disposaran de torns d'accés, amb identificació del treballador / visitant i amb videovigilància permanent.

- Es realitzaran llistats complets i detallats d'entrades i sortides, tant de treballadors, com dels propis actius (portàtils, smartphones...) que siguin propietat de l'empresa.

- Els dispositius de seguretat seran revisats periòdicament per poder assegurar que el seu funcionament és el més adequat i el més actual, segons les noves tècniques que vagin apareixent en el mercat.

- Les possibles incidències en la seguretat física, perimetral o en el control d'accés seran reportats en el formulari d'incidències, i seran automàticament enviats al departament corresponent per poder realitzar la immediata reparació o la proposta de millora necessària.

- Les contrasenyes d'accés han de tenir un nombre mínim de 8 caràcters alfanumèrics, que incloguin majúscules i minúscules conjuntament. Aquestes contrasenyes han de ser modificades cada 3 mesos obligatòriament.

2.2. Procediment d'auditories internes:

Encapçalament del document:

Codi	Auditories_Internes_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	Versió	Autor	Descripció
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de les auditories internes.
	....		
	....		

2.2.1. Introducció:

En el document del procediment d'auditories internes s'especifica la forma i manera de realització de les auditories que l'organització haurà de realitzar per poder mantenir al llarg dels anys la vigència de la certificació, especificant la forma i requisits d'aquestes auditories.

2.2.2. Abast, missió i objectius de l'auditoria interna:

- El principal objectiu de l'auditoria serà la planificació, execució i creació de resultats i informes del SGSI de l'empresa, així com el seguiment de la seva seguretat.

- L'auditoria tindrà l'abast de tot el sistema d'informació de l'empresa i elements relacionats amb la implantació, correcció i millora de la mateixa. Entre d'altres, s'hauran de controlar les vulnerabilitats detectades, i la correcta implantació dels controls i indicadors que s'hagin fet servir per la implantació de la norma. Així mateix també s'haurà de confirmar que es disposa de tota la documentació, i que aquesta està suficientment actualitzada, tenint en compte la normativa ISO.

- També és important que l'equip auditor sigui independent, així les conclusions i anàlisis seran més objectius.

2.2.3. Procediment d'auditoria interna:

- Primerament, l'equip auditor necessita el compromís de direcció per poder portar a terme l'auditoria, amb el compromís per escrit.

- Aquesta auditoria s'hauria de realitzar com a mínim un cop l'any, per poder tenir resultats satisfactoris per la seguretat dels sistemes de l'empresa.

- S'hauran de planificar degudament totes les tasques d'auditoria que s'han de realitzar, per interferir el mínim possible en el correcte desenvolupament de les tasques del propis treballadors de l'empresa.

- Els responsables hauran d'informar als departaments o personal involucrat en l'auditoria de les dades i hores en que es produirà, per poder ajudar a l'equip a realitzar la seva tasca més eficientment.

- Per a poder realitzar el procés d'autoria, l'equip encarregat inicialment ha de recollir el màxim d'informació dels diferents empleats seleccionats, i amb els quals haurà de mantenir una entrevista, per exemple, amb el responsable de seguretat de l'empresa, i amb els diferents caps de departament.

- L'equip auditor també haurà de revisar la diferent documentació de que disposi l'empresa, dels diferents elements, normatives, i polítiques de que disposi.

- L'equip auditor realitzarà l'auditoria conforme al pla dissenyat, i en realitzarà els informes corresponents al finalitzar, posant-los en coneixement dels caps, i personal responsable de l'empresa.

- Es realitzaran i comprovaran tots els llistats de verificació de l'auditoria relacionats amb requeriments del sistema i la verificació dels diferents controls de seguretat.

- Si l'equip auditor realitza una auditoria dels controls de seguretat implantats haurà de auditar i comprovar el compliment, entre d'altres, la política de seguretat, l'organització, la seguretat dels recursos humans, els actius de l'empresa, la seguretat física, ambiental i de accés, les comunicacions, els processos, el manteniment dels sistemes d'informació, els incidents que s'hagin produït, i els plans de continuïtat del negoci, o la conformitat.

- L'equip realitzarà un informe complet amb totes les dades recollides, les no conformitats (amb les diferents classificacions, de greu, lleu, de amb possibilitat de millora) i les observacions detectades o punts positius del sistema, així mateix també inclourà en l'informe les recomanacions de possibles nous projectes que puguin sorgir segons els resultats obtinguts i que puguin ajudar a millorar notablement la seguretat del sistema de l'empresa.

- L'informe serà enviat a direcció, i mitjançant una reunió s'informarà del seu contingut, resultats i conclusions, per tal de que l'equip de direcció pugui realitzar accions correctives o de millora, en cas de ser necessari.

- També s'haurà de realitzar un seguiment i millora continua dels resultats obtinguts, i sobretot de les no conformitats, de forma que el sistema pugui ser certificat o pugui mantenir la certificació durant els anys.

2.2.4. Equips d'auditoria:

- Es conformarà un equip per realitzar les corresponents auditories, format per membres interns i sobretot externs a l'organització, independents a l'organització.

- L'equip d'auditoria disposarà d'un conjunt de membres, que realitzaran l'auditoria pròpiament dita, i un auditor en cap, que s'encarregarà de preparar el pla d'auditoria, coordinar els membres, informar i liderar el procés, entre d'altres.

- L'equip haurà d'estar format per persones qualificades i amb experiència en l'àmbit de les auditories, amb capacitats innates de comunicació, per a la realització d'entrevistes, o qüestionaris, capacitat de síntesi, per a la realització d'informes, i coneixement extens de les normatives ISO que s'estan utilitzant.

2.3. Gestió d'indicadors:

Encapçalament del document:

Codi	Gestió_Indicadors_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	Versió	Autor	Descripció
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de gestió d'indicadors.
	....		
	....		

2.3.1. Introducció:

En aquest document s'especificarà la sistemàtica per a realitzar les mesures dels diferents indicadors de que disposarà el sistema de l'organització.

2.3.2. Components dels indicadors:

El nostre sistema d'informació disposa de diferents indicadors de seguretat que ens permeten millorar l'eficiència dels nostres controls que tenim implantats en l'empresa. Cada control de la nostra organització haurà de disposar d'algun indicador que permeti saber com funciona el control concret, i que les auditories puguin mesurar com funciona el SGSI.

El indicadors, disposen d'una sèrie de característiques que permeten identificar-los i documentar-los en el nostre sistema. Com a principals en podem destacar, el seu nom, una breu descripció de l'indicador i la seva mesura, els controls als que fa referència, així com una forma de mesurament, una freqüència i unitats de mesura, amb valors esperats i valors límits (mínims i màxims on generar alertes de funcionament erroni del control), i els responsables del seu mesurament periòdic.

Per tant, disposarem dels diferents controls, amb el conjunt de indicadors, i amb els diferents valors de si la mesura obtinguda pel equip auditor o pel responsable de la mesura periòdica és tolerable o no per cada indicador, amb l'objectiu de la millora contínua.

2.3.3. Tipologies d'indicadors:

Dins dels indicadors que la nostre empresa podria utilitzar en podem trobar de diferents tipologies segons les categories de la normativa, tot seguit en podem veure una mostra:

- Política de Seguretat: Nombre de controls de la ISO aplicables, nombre de revisions de la política, percentatge d'adopció entre els treballadors, o canvis realitzats en un període de temps.

- Organització de la seguretat de la informació: Nombre d'incidències detectades a la normativa, nombre d'auditories realitzades, nombre de contactes realitzats en terceres parts.

- Gestió d'actius: Nombre de revisions de l'inventari d'actius, actius identificats amb risc, percentatge d'amenaces en els actius, o percentatge de dades sensibles.

- Seguretat del personal: Penetració de la seguretat entre els treballadors, nombre d'hores de formació en seguretat, incidències detectades entre treballadors, nombre d'actius robats / perduts, percentatge de lloc de treball net o desatès.

- Seguretat física i de l'entorn: Percentatge de intrusions en el sistema físic, percentatge de obsolescència tecnològica, o nombre de revisions de manteniment realitzades.

- Gestió de comunicacions i operacions: Efectivitat dels proveïdors de comunicacions, percentatge de còpies de seguretat realitzades, percentatge d'actualitzacions portades a terme, percentatge de vulnerabilitats de les comunicacions, o nombre d'incidents de seguretat de les comunicacions.

- Control d'accés: Percentatge de intents d'accés, efectivitat dels controls d'accés, percentatge de treballadors amb accés a llocs sensibles.

- Seguretat d'adquisició, desenvolupament i manteniment de sistemes d'informació: Percentatge de processos modificats respecte a la normativa, percentatge de desenvolupaments i manteniments realitzats, nombre d'adquisicions realitzades.

- Gestió d'incidències de seguretat: Nombre d'incidències registrades, i nombre de incidències solucionades respecte a les no solucionades, o cost dels incidents generats.

- Gestió de la continuïtat del negoci: Percentatge de desplegament del pla de continuïtat del negoci, o efectivitat del pla de continuïtat.

- Conformitat: Efectivitat de les auditories realitzades, percentatge de recomanacions realitzades, nombre de normatives legals noves incloses, o temps de resolució de les no conformitats detectades.

2.4. Procediment de revisió per direcció:

Encapçalament del document:

Codi	Revisió_Direcció_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	Versió	Autor	Descripció
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de revisió de direcció.
	....		
	....		

2.4.1. Introducció:

En aquest document s'especificarà el procediment pel qual direcció de l'organització realitzarà la revisió de les qüestions més importants referents a la seguretat del nostre sistema d'informació, d'una manera que sigui planificada, i segons la normativa ISO 27001 i 27002.

2.4.2. Missió, objectiu i abast del procés i periodicitat:

- El procediment de revisió per part de direcció inclou tots els possibles elements que han estat implantats en el nostre sistema d'informació i que s'han avaluat, i que possiblement tenen punts de millora, o nous objectius que cobrir, i que, per tant, l'equip de direcció n'ha de donar la seva conformitat.

- Els elements que s'inclouen en l'abast ja hauran estat auditats, i per tant, l'equip de direcció, en disposarà dels corresponents informes, per poder veure on falla, o quins elements es comporten com es degut, i quins punts del sistema necessiten una millora o correcció.

- La periodicitat de la revisió coincidirà amb l'auditoria realitzada cada any, per tant la revisió es realitzarà anualment.

2.4.3. Procediment de revisió de direcció:

- Es important que l'equip de direcció sàpiga l'estat actual del seu SGSI, que tingui els resultats disponibles d'auditories anteriors, si existeixen, i que tingui la previsió d'inversió que pot voler destinar a seguretat a curt, mitjà i llarg termini,

per poder afrontar el procés de revisió amb tota la informació disponible, i per tant, podent prendre millors decisions i més contrastades.

- També pot ser molt útil, per la pressa de decisions, disposar d'unes estadístiques de les diferents incidències que l'equip de seguretat de l'empresa hagi detectat en els últims temps.

- Un cop l'equip auditor ha realitzat els corresponents informes amb els diferents elements analitzats i amb els diferents controls del sistema d'informació analitzats, tant de seguretat física, com lògica, aquests estaran a disposició de direcció per a la seva revisió.

- La direcció realitzarà l'anàlisi dels informes un cop cada any, coincidint amb la auditoria. I s'informarà de la mateixa a tots els departaments i òrgans de la nostre empresa que hi estiguin involucrats, mitjançant una acurada planificació.

- Els informes que necessitarà direcció, entre d'altres, hauran d'incloure la revisió d'auditoria de les diferents polítiques de seguretat, les normatives, els riscos, les amenaces, les vulnerabilitats detectades, així com el control de tota la documentació aportada pels diferents departaments, i dels controls de seguretat que hagin estat implantats, i que necessiten ser revisats per poder seguir el principi de millora contínua.

- L'equip de direcció, un cop finalitzada l'auditoria, disposaran dels següents elements de decisió:

    - Resultats de l'auditoria interna, i conclusions de l'equip auditor.
    - Informació detallada del sistema d'informació, amb els punts de millora o correcció.
    - Estat actual del sistema, amb possibles mesuraments dels indicadors.
    - Informació detallada dels resultats de les entrevistes amb els caps de departament.
    - Possibles projectes de millora dels sistemes d'informació o de la pròpia seguretat dels mateixos.
    - Punts que funcionen correctament.
    - Requeriments de seguretat o legals, per novetats en legislacions o en seguretat.
    - Obligacions amb tercers o amb contractes existents.
    - Inversió disponible per possibles nous projectes de millora.
    - No conformitats a la norma detectades que han de ser arreglades.

- Finalment, l'equip de direcció farà el tancament de l'auditoria anual, amb la previsió dels nous objectius del seu sistema, i amb les conclusions del resultat de l'auditoria, tenint en compte tots els punts de millora contínua.

2.5. Gestió de rols i responsabilitats:

Encapçalament del document:

Codi	Rols_Responsabilitats_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	Versió	Autor	Descripció
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de rols i responsabilitats.
	....		
	....		

2.5.1. Introducció:

En aquest document s'especificarà l'equip que s'encarregarà de crear, mantenir, supervisar i millorar el sistema de informació, i la seva seguretat. Aquest equip s'anomena comitè de seguretat.

2.5.2. Missió i objectius de rols i responsabilitats:

En la nostre empresa podrem distingir tres tipologies de rols que poden tenir els diferents usuaris dels diferents departaments, que són el rol d'usuari (cadascun dels treballadors dels diferents departaments de l'empresa), el rol de propietari (responsables dels diferents departaments), o podem trobar el rol d'administració (personal TIC).

Amb el tema de les responsabilitats, s'establiran un conjunt de responsabilitats segons la tipologia d'usuari, i que els diferents conjunts de treballadors han de respectar. Per exemple, podem trobar la responsabilitat de complir amb les diferents polítiques o normatives de seguretat de les empreses, que tindran tots els treballadors de l'empresa.

Així mateix, podem trobar que els propietaris hauran de gestionar els drets d'accés, així com la seva confidencialitat. Els administradors tindran alguns drets i deures per poder administrar els sistemes segons les necessitats dels propis propietaris, assegurant la informació, el control d'accés, i el seu correcte manteniment. I finalment, els usuaris els correspon, com he assenyalat, complir amb totes les normatives vigent en l'empresa, així com utilitzar les seves credencials adequadament i mantenint la confidencialitat de les dades o sistemes que utilitzen en la seva tasca diària.

Si en centrem a comentar els principals rols i responsabilitats relacionats amb la seguretat del sistema d'informació podem trobar els següents més destacats:

2.5.3. Comitè de seguretat:

- El comitè de seguretat, que serà format per personal qualificat de l'empresa i que representin a la seguretat de l'empresa, vetllaran pel correcte funcionament de la seguretat de l'empresa, amb estreta comunicació amb el responsable de seguretat de l'empresa.

- Així mateix aquest comitè també implantaran les directrius, rols i funcions de seguretat que indiqui el comitè de direcció, i també hauran de validar els riscos i accions de millora, validar el pla de seguretat i el pla de continuïtat del negoci, i fer-ne el seu seguiment. També vetllaran pel compliment legal i promouran la seguretat i la formació dels usuaris, així com revisaran les incidències més destacades que hagin ocorregut en l'empresa.

2.5.4. Comitè de direcció:

- El comitè de direcció estarà format per professionals d'alta direcció de l'empresa i que siguin representatius del conjunt d'empleats, i que s'encarregaran de vetllar i de prendre les diferents decisions estratègiques pel conjunt de l'empresa. Com a eines, disposaran de tots els informes de les diferents auditories realitzades per l'equip auditor. Un punt molt important és el compromís de la direcció en els diferents projectes de seguretat que hagin de realitzar-se en l'empresa, així com també són importants per poder aprovar pressupostos estratègics i inversions necessàries en seguretat.

- També seran els encarregats de nombrar el comitè de seguretat, dotar-lo de recursos i establir-ne les directrius necessàries, així com també, hauran d'aprovar les directrius i plans de seguretat més importants i realitzar-ne el seguiment en termes de direcció.

2.5.5. Responsable de seguretat del sistema:

- El responsable de seguretat serà el professional designat per l'empresa, amb els suficients coneixements de seguretat i d'informàtica, i amb l'experiència adequada per dur a terme aquest càrrec. Assumirà el control d'incidències, assegurar-se que es compleixen les diferents normatives i polítiques de seguretat, realitzar millores en la seguretat, mantenir-la, i realitzar consultoria i formació als usuaris que ho requereixin.

- També serà l'encarregat de implantar el que indiqui el comitè de seguretat, promovent la seguretat de la informació, i proposant nous objectius, i ajudant a mantenir i desenvolupar el marc normatiu de l'empresa en seguretat. Així com també revisarà i coordinarà periòdicament l'estat de seguretat de l'empresa en plans, tècniques i metodologies.

2.5.6. Personal del departament TIC:

- Encara que aquesta tipologia de treballadors no seria especialment centrada només en seguretat, si que té un paper primordial en la resolució de les incidències que els diferents empleats de l'empresa observen o detecten, així

com també tenen un paper tècnic molt important del manteniment dels sistemes de l'empresa, i amb coordinació amb el responsable de seguretat. Fet que també els fa esdevenir una peça clau indirectament en la seguretat de l'empresa.

- Seran també els encarregats de implantar la seguretat en els sistemes, realitzar-ne les accions de millora, i gestionar les vulnerabilitats detectades, així com també, realitzaran els canvis de hardware i software que siguin necessaris, i col·laborar amb les revisions i auditories de seguretat que l'empresa realitzi

2.5.7. L'equip auditor:

- Serà un equip format per personal qualificat i amb l'experiència suficient per poder realitzar les tasques d'auditoria periòdica de l'empresa. Per tal de mesurar i poder tenir controlada la seguretat del sistema, així com per vetllar pel correcte funcionament i compliment dels controls i indicadors que l'empresa té implantats. Han de ser persones amb una gran capacitat comunicativa i de síntesi i domini de les situacions adverses.

2.6. Metodologia d'anàlisi de riscos:

Encapçalament del document:

Codi	Metodologia_AnalisiRiscos_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	**Versió**	**Autor**	**Descripció**
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de la metodologia de anàlisi de riscos.
	....		
	....		

2.6.1. Introducció:

Aquest document inclourà la sistemàtica que s'haurà de seguir per a calcular el risc dels actius, amenaces i vulnerabilitats de l'organització.

2.6.2. Objectius i metodologia Magerit:

En aquesta empresa utilitzarem una de les metodologies que existeixen en l'anàlisi de riscos, es tracta de Magerit v3, una metodologia per l'anàlisi i gestió de riscos en sistemes d'informació, elaborada per l'Administració Pública.

Magerit té com a principals objectius, conscienciar als responsables dels riscos de les seves empreses, i de la important necessitat de saber-los gestionar correctament, així com també ens ofereix una metodologia sistemàtica per detectar i analitzar aquests riscos, realitzar-ne un tractament, i tenir el sistema a punt per poder ser certificat o auditat, en el moment que sigui necessari.

Dins de la metodologia de Magerit podem diferenciar dos processos: l'anàlisi de riscos, que ens permet determinar-los, i el seu tractament, per evitar possibles incidències en un present o futur.

Breument, cal dir que Magerit considera els següents elements, en el moment de realitzar l'anàlisi de riscos: els actius, les amenaces, les salvaguardes, el seu impacte i el risc, o probabilitat que passi l'amenaça concreta.

2.6.3. Fases d'anàlisi de riscos Magerit:

A. Obtenció de dades dels processos del sistema.

B. Establiment de paràmetres, amb la dimensió.
C. Anàlisi dels actius del sistema, amb la seva interrelació i el seu valor.
D. Detecció de les amenaces a que estan subjectes aquests actius.
E. Determinar quines salvaguardes hi ha disponibles i la seva eficàcia.
F. Estimar l'impacte que tindria sobre l'actiu si es materialitza l'amenaça.
G. Influencia de controls de seguretat
H. Estimar el risc de l'amenaça.

També haurem d'establir unes valoracions mitjançant l'establiment de valors quantitatius, als actius, per exemple, per poder-ne realitzar valoracions posteriors. Podríem tenir unes escales d'importància com les següents:

- Valor molt alt > A (>250.000€)
- Valor alt entre B i C (entre 250.000€ i 50.001€)
- Valor mitjà entre D i E (entre 50.000€ i 10.001€)
- Valor baix entre F i G (entre 10.000€ i 1.000€)
- Valor molt baix < H (menys de 1.000€)

Cal tenir en compte que alguns d'aquests elements analitzats poden estar relacionats entre si, i per tant, el seu valor pot ser superior a l'habitual en alguns casos.

Pel que fa referència a les dimensions de seguretat, ens permetrà determinar la seva importància en el sistema, per exemple, pels actius, i segons l'enllaç de MAGERIT, inclòs en la bibliografia, podem trobar: la disponibilitat, la integritat, la traçabilitat, la confidencialitat o l'autenticitat.

Si volem valorar les amenaces segons la freqüència de materialització de l'amenaça, podríem trobar el següent:

- Freqüència molt alta: diàriament
- Freqüència alta: mensualment
- Freqüència mitjana: anualment
- Freqüència baixa: cada diversos anys
- Freqüència molt baixa: casi mai es donaria

També podem realitzar la valoració per impactes que té en l'actiu si es produeix la incidència i no l'hem pogut aturar, i que hem de valorar tenint en compte el resultat, l'efecte produït i el valor econòmic que ha generat l'impacte:

- Impacte molt alt 100%
- Impacte alt 75%
- Impacte mitjà 50%
- Impacte baix 25%
- Impacte molt baix 5%

Podem realitzar la valoració de l'efectivitat de les salvaguardes de seguretat:

- Efectivitat molt alta 90% (mai tindria una efectivitat real del 100%)
- Efectivitat alta 75%

- Efectivitat mitjana 50%
- Efectivitat baixa 25%
- Efectivitat molt baixa 5%

També podem tenir en compte que les diferents amenaces que poden actuar en el nostre sistema poden provenir de diferents llocs, com són, desastres naturals, accidents, errors no intencionats i errors intencionats (o també els podem dir atacs), que aquests poden ser locals o remots.

Les salvaguardes utilitzades poden ser de dos tipologies, preventives, que redueixen les vulnerabilitats i correctives, que ens redueixen l'impacte de l'amenaça.

Posteriorment, amb l'estimació del risc, s'analitza la forma en que aquests riscos de l'empresa poden ser reduïts amb les salvaguardes proposades. Per tant, ens permetrà prendre les decisions correctes sobre si un risc concret ha de ser reduït, transferit, o acceptat per l'empresa. Ja que moltes vegades el seu cost d'actuació sobre el risc pot arribar a ser molt alt, i no totes les empreses disposen de grans inversions disponibles.

2.7. Declaració d'aplicabilitat:

Encapçalament del document:

Codi	Declaració_Aplicabilitat_SGSI_01
Versió	V.1
Autor	Jordi Miró Amigó
Revisió	R.1.
Data de Publicació	1 de Novembre de 2013
Aprovació	Pendent
Data d'aprovació	Pendent
Confidencialitat	Mitjana

Historial de revisions:

Data	**Versió**	**Autor**	**Descripció**
1 de Novembre de 2013	V.1	Jordi Miró Amigó	Nova creació del document de la declaració d'aplicabilitat.
	....		
	....		

2.7.1. Introducció:

La declaració d'aplicabilitat ens inclou els diferents controls de seguretat de l'organització, amb informació de l'aplicabilitat (aplica o no aplica) i amb un apartat d'observacions per poder determinar el seu estat, o si es disposa de la documentació relacionada amb cada cas.

Tot seguit podem veure el quadre d'anàlisis d'aplicabilitat:

ANÀLISIS D'APLICABILITAT ISO 27001 - 27002		
TIPUS DE CONTROL ISO	**APLICA ?**	**OBSERVACIONS**
5. Política de seguretat		
5.1. Política de seguretat de la informació		
5.1.1. Document de política de seguretat de la informació	**APLICA**	L'empresa disposa del document però no s'actualitza ni revisa.
5.1.2. Revisió de la política de seguretat de la informació	**APLICA**	Es necessita una actualització i revisió de la política de seguretat.
6. Aspectes organitzatius de la seguretat de la informació		
6.1. Organització interna		
6.1.1. Compromís de la direcció amb la seguretat de la informació	**APLICA**	La direcció està convençuda i compromesa amb la seguretat, vol disposar de totes les mesures necessàries, tenint sempre en compte la relació cost/eficàcia
6.1.2. Coordinació de la seguretat de la informació	**APLICA**	El departament de IT és el responsable de la coordinació en temes de seguretat.

6.1.3. Assignació de responsabilitats relatives a la seguretat de la informació	**APLICA**	El departament de IT és l'encarregat de les tasques de seguretat.
6.1.4. Procés d'actualització de recursos pel tractament de la informació	**APLICA**	No està correctament especificats els rols de seguretat.
6.1.5. Acords de confidencialitat	**APLICA**	Existeixen acords de confidencialitat pels treballadors de l'empresa
6.1.6. Contacte amb les autoritats	**APLICA**	En el cas que hi hagués algun problema que requerís el contacte amb autoritats és realitzaria, però no està especificat.
6.1.7. Contacte amb grups d'especial interès	**NO APLICA**	No s'ha especificat cap contacte amb grups d'especial interès.
6.1.8. Revisió independent de la seguretat de la informació	**NO APLICA**	No s'ha tingut en compte que és realitzi una revisió independent de la seguretat de la informació.
6.2. Tercers		
6.2.1. Identificació dels riscos derivats de l'accés de tercers	**APLICA**	No estan especificats els riscos d'accés de tercers.
6.2.2. Tractament de la seguretat en la relació amb els clients	**APLICA**	S'apliquen diferents nivells de seguretat segons les dades de que es disposen dels clients.
6.2.3. Tractament de la seguretat en contractes amb tercers	**APLICA**	No s'ha especificat.
7. Gestió d'actius		
7.1. Responsabilitat sobre els actius		
7.1.1. Inventari d'actius	**APLICA**	Es disposa d'un inventari d'actius, però no està actualitzat ni revisat.
7.1.2. Propietat dels actius	**APLICA**	S'especifica en l'inventari la propietat de cada actiu.
7.1.3. Ús acceptable dels actius	**APLICA**	Existeix una política que els usuaris han d'acceptar i respectar.
7.2. Classificació de la informació		
7.2.1. Directrius de classificació	**APLICA**	Es classifica la informació segons la seva sensibilitat o segons el seu nivell crític.
7.2.2. Etiquetat i manipulat de la informació	**APLICA**	S'utilitza un gestor documental per la documentació de que disposa l'empresa.
8.Seguretat lligada als recursos humans		
8.1. Abans de la feina		
8.1.1. Funcions i responsabilitats	**APLICA**	Es contracta als treballadors segons els seus rols o perfils de funcions.
8.1.2. Investigació d'antecedents	**APLICA**	El departament de RRHH s'encarrega de la tasca.
8.1.3. Termes i condicions de contractació	**APLICA**	En el moment de la contractació els empleats firmen les condicions i la

		confidencialitat.
8.2. Durant la feina		
8.2.1. Responsabilitats de la direcció	**APLICA**	S'apliquen uns rols de responsabilitat determinats.
8.2.2. Conscienciació, formació i capacitació en seguretat de la informació	**APLICA**	L'empresa dedica alguna part del pressupost a la formació en seguretat pels seus empleats.
8.2.3. Procés disciplinari	**APLICA**	Es pressuposa que existeix, però no se'n coneix el contingut escrit.
8.3. Finalització de la feina o canvi de lloc de treball		
8.3.1. Responsabilitat de finalització o canvi	**APLICA**	S'apliquen els rols de responsabilitat determinats.
8.3.2. Devolució d'actius	**APLICA**	Un cop finalitzat, s'han de realitzar la devolució d'actius que han sigut entregats a l'empleat.
8.3.3. Retirada de drets d'accés	**APLICA**	El departament de IT retira els drets d'accessos al sistema de l'empleat donat de baixa.
9. Seguretat física i de l'entorn		
9.1. Àrees segures		
9.1.1. Perímetre de seguretat física	**APLICA**	Existeixen diferents mesures de seguretat exterior, com poden ser càmeres, sensors i vigilants.
9.1.2. Controls físics d'entrada	**APLICA**	El control físic d'entrada es realitza mitjançant una targeta unipersonal.
9.1.3. Seguretat d'oficines, despatxos i instal·lacions	**APLICA**	Les dependències amb material sensible, com servidors, està controlat per codis PIN, i sensors de moviment.
9.1.4. Protecció contra les amenaces externes i d'origen ambiental	**APLICA**	El subministrament elèctric disposa de SAI's de suport.
9.1.5. Treball en àrees segures	**APLICA**	No es pot assegurar que siguin àrees segures, ja que podrien accedir-hi altres persones, amb el mateix codi PIN.
9.1.6. Àrees d'accés públic i de càrrega i descarrega	**NO APLICA**	No existeix una àrea especifica de càrrega i descarrega.
9.2. Seguretat dels equips		
9.2.1. Distribució i protecció dels equips	**APLICA**	Algunes dependències disposen d'accés amb PIN, els despatxos normals no.
9.2.2. Instal·lacions de subministrament	**APLICA**	El subministrament elèctric disposa de SAI's de suport.
9.2.3. Seguretat del cablejat	**APLICA**	No s'ha especificat.
9.2.4. Manteniment dels equips	**APLICA**	El manteniment el realitza el departament de IT, però s'hauria de millorar.
9.2.5. Seguretat dels equips de	**APLICA**	No existeix una seguretat dels

fora les instal·lacions		equips que surten de les instal·lacions, excepte per l'ús de VPN's.
9.2.6. Reutilització o retirada segura d'equips	**APLICA**	Un cop es retiren els equips es dipositen a empreses residus, però no es realitza un format a baix nivell, només un de normal.
9.2.7. Retirada de materials propietat de l'empresa	**APLICA**	Es necessita omplir un imprès i aquest ha de ser autoritzat.
10. Gestió de comunicacions i operacions		
10.1.Responsabilitats i procediments d'operació		
10.1.1. Documentació dels procediments d'operació	**APLICA**	No estan completament documentats.
10.1.2. Gestió de canvis	**APLICA**	Els canvis són duts a terme de manera definida.
10.1.3. Segregació de tasques	**APLICA**	Es segreguen tasques segons els especialistes.
10.1.4. Separació dels recursos de desenvolupament, prova i operació	**APLICA**	Es compleix aquesta separació de recursos segons la seva tipologia.
10.2. Gestió de la provisió de serveis per tercers		
10.2.1. Provisió de serveis	**NO APLICA**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.2.2. Supervisió i revisió dels serveis oferts per tercers	**NO APLICA**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.2.3. Gestió del canvi en els serveis oferts per tercers	**NO APLICA**	No és té contractat cap prestació de serveis per terceres parts externes a l'empresa.
10.3. Planificació i acceptació del sistema		
10.3.1. Gestió de capacitats	**APLICA**	S'avalua la capacitat de la infraestructura periòdicament.
10.3.2. Acceptació del sistema	**APLICA**	Es realitza la acceptació quan es comprova que tot funciona correctament.
10.4. Protecció contra el codi maligne i descarregues		
10.4.1. Controls contra el codi maligne	**APLICA**	Es disposa de programari de detecció de virus i programaris malignes que s'actualitza diàriament.
10.4.2. Controls contra el codi descarregat en el client	**APLICA**	Es disposa d'unes normes que prohibeixen el codi descarregat de tercers en l'empresa si no se sap l'origen confiable.
10.5. Copies de seguretat		
10.5.1. Copies de seguretat de la informació	**APLICA**	Es realitza periòdicament un backup de dades dels servidors i dels discs durs del sistema, però no

		de les dades locals dels equips personals dels treballadors.
10.6. Gestió de la seguretat de les xarxes		
10.6.1. Controls de xarxa	**APLICA**	La xarxa es controlada per programaris de monitoreig, tipus Nagios, i programaris de firewall.
10.6.2. Seguretat dels serveis de xarxa	**APLICA**	Els programaris de seguretat controles els diferents serveis de la xarxa, per assegurar-ne el correcte funcionament.
10.7. Manipulació dels suports		
10.7.1. Gestió de suports extraïbles	**APLICA**	No existeix actualment.
10.7.2. Retirada de suports	**APLICA**	Si són suports de disc durs és realitza un format, però no de baix nivell.
10.7.3. Procediments de manipulació de la informació	**APLICA**	La informació es classifica i es manipula segons si es critica i segons els rols dels treballadors.
10.7.4. Seguretat de la documentació del sistema	**APLICA**	La documentació dels sistema en té accés els perfils adequats, del gestor documental.
10.8. Intercanvi de informació		
10.8.1. Polítiques i procediments de intercanvi de informació	**APLICA**	No està especificat.
10.8.2. Acords de intercanvi	**APLICA**	No estan especificats.
10.8.3. Suports físics en transit	**APLICA**	No està especificat.
10.8.4. Missatgeria electrònica	**APLICA**	S'utilitza per tasques internes de treballadors de la pròpia empresa.
10.8.5. Sistemes de informació empresarial	**APLICA**	Es disposa d'un sistema de informació empresarial amb gestor documental.
10.9. Serveis de comerç electrònic		
10.9.1. Comerç electrònic	**APLICA**	El comerç electrònic del portal web està especificat.
10.9.2. Transaccions en línia	**APLICA**	S'utilitza un sistema de transaccions en línia segures.
10.9.3. Informació públicament disponible	**APLICA**	S'utilitzen sistemes de seguretat per evitar intrusions.
10.10. Supervisió		
10.10.1. Registres d'auditoria	**APLICA**	No s'han realitzat auditories, però el sistema disposa d'un sistema de logs.
10.10.2. Supervisió de l'ús del sistema	**APLICA**	El propi sistema monitoritza l'ús del sistema, per detectar comportaments inadequats
10.10.3. Protecció de la informació dels registres	**APLICA**	Els logs estan protegits per les pròpies eines del sistema.

10.10.4. Registres d'administració i operació	**APLICA**	Els registres queden guardats al servidor.
10.10.5. Registre de fallades	**APLICA**	Les incidències queden registrades, i posteriorment a la solució, es documenten i arxiven.
10.10.6. Sincronització de rellotge	**APLICA**	El servidor disposa de la sincronització de rellotge.
11. Control d'accés		
11.1. Requisits de negoci pel control d'accés		
11.1.1. Política de control d'accés	**APLICA**	L'accés es realitza mitjançant una política de control d'accés a les instal·lacions critiques.
11.2. Gestió d'accés d'usuari		
11.2.1. Registre d'usuari	**APLICA**	Existeix un procediment de registre d'usuaris.
11.2.2. Gestió de privilegis	**APLICA**	Existeix una gestió dels privilegis dels diferents tipus o perfils d'usuaris.
11.2.3. Gestió de contrasenyes d'usuari	**APLICA**	Existeix una gestió de les contrasenyes dels diferents perfils d'usuaris.
11.2.4. Revisió dels drets d'accés d'usuari	**APLICA**	Es revisen els drets d'accés dels usuaris segons els seus perfils o canvis de perfils.
11.3. Responsabilitats d'usuari		
11.3.1. Ús de contrasenyes	**APLICA**	Existeix una política d'ús i creació de contrasenyes.
11.3.2. Equip d'usuari desatès	**APLICA**	Existeix una normativa antiga, però necessita una revisió i recordar-la als usuaris.
11.3.3. Política de lloc de treball buit i pantalla neta	**APLICA**	Existeix una normativa antiga, però necessita una revisió i recordar-la als usuaris.
11.4. Control d'accés a xarxa		
11.4.1. Política d'ús dels serveis de xarxa	**APLICA**	Existeix una política d'ús dels serveis de xarxa, però necessita una revisió.
11.4.2. Autentificació d'usuari per connexions externes	**APLICA**	Es disposa d'accés per VPN.
11.4.3. Identificació dels equips en les xarxes	**APLICA**	Els equips queden registrats i identificats en les xarxes en les que es connecten.
11.4.4. Diagnòstic remot i protecció dels ports de configuració	**APLICA**	Les eines del sistema permeten un diagnòstic remot i protecció de ports.
11.4.5. Segregació de les xarxes	**APLICA**	Existeixen diferents xarxes segregades segons funcions.
11.4.6. Control de la connexió a la xarxa	**APLICA**	Les connexions a la xarxa estan controlades per programari del

		sistema.
11.4.7. Control d'encaminament (Routing) de xarxa	**APLICA**	El tràfic passa per firewalls i protocols que controlen la xarxa.
11.5. Control d'accés al sistema operatiu		
11.5.1. Procediments segurs d'inici de sessió	**APLICA**	Es disposa de noms d'usuari, contrasenyes, i certificats a disposició dels diferents perfils d'usuaris.
11.5.2. Identificació i autentificació d'usuari	**APLICA**	Es realitza una identificació i autentificació dels diferents perfils d'usuaris.
11.5.3. Sistema de gestió de contrasenyes	**APLICA**	Es realitza una gestió de les diferents contrasenyes dels sistemes.
11.5.4. Ús dels recursos del sistema	**APLICA**	Es controla mitjançant programari l'ús dels diferents recursos del sistema.
11.5.5. Desconnexió automàtica de sessió	**APLICA**	Al cap d'un temps determinat d'inactivitat es desconnecta la sessió.
11.5.6. Limitació de temps de connexió	**APLICA**	No existeix actualment.
11.6. Control d'accés a les aplicacions i a la informació		
11.6.1. Restricció de l'accés a la informació	**APLICA**	Es pot restringir l'accés a la informació de que disposen els servidors, però la informació en equips personals no sempre es tan segura.
11.6.2. Aïllament de sistemes sensibles	**APLICA**	Els sistemes més sensibles estan aïllats de la resta de la xarxa.
11.7. Ordinadors portàtils i teletreball		
11.7.1. Ordinadors portàtils i comunicacions mòbils	**APLICA**	No existeix un control eficaç de les comunicacions mòbils i portàtils.
11.7.2. Teletreball	**APLICA**	Es pot realitzar mitjançant una VPN.
12. Adquisició, desenvolupament i manteniment dels sistemes de informació		
12.1. Requisits de seguretat dels sistemes de informació		
12.1.1. Anàlisi i especificació dels requisits de seguretat	**APLICA**	Es comproven que en els canvis i nous desenvolupaments es segueixin els requisits de seguretat necessaris en cada cas.
12.2. Tractament correcte de les aplicacions		
12.2.1. Validació de les dades d'entrada	**APLICA**	El programari valida que les dades d'entrada siguin correctes.
12.2.2. Control de processament intern	**APLICA**	El programari valida el processament intern.
12.2.3. Integritat dels missatges	**APLICA**	S'assegura la integritat dels missatges que el programari envia.
12.2.4. Validació de les dades	**APLICA**	El programari valida les dades de

de sortida		sortida.
12.3. Controls criptogràfics		
12.3.1. Política d'ús dels controls criptogràfics	**APLICA**	No s'especifica documentalment.
12.3.2. Gestió de claus	**APLICA**	No s'especifica documentalment.
12.4. Seguretat dels arxius del sistema		
12.4.1. Control del programari en explotació	**APLICA**	Existeixen procediments que han de ser revisats.
12.4.2. Protecció de les dades de prova del sistema	**APLICA**	Existeixen procediments que han de ser revisats.
12.4.3. Control d'accés al codi font dels programes	**APLICA**	El accés al codi font dels programes està protegit.
12.5. Seguretat en el procés de desenvolupament i suport		
12.5.1. Procediments de control de canvis	**APLICA**	Es realitzen procediments de control de canvis.
12.5.2. Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	**APLICA**	Es comprova el bon funcionament després d'efectuar canvis en el sistema operatiu.
12.5.3. Restriccions als canvis en els paquets de programari	**APLICA**	No existeixen restriccions concretes als canvis en els paquets de programari.
12.5.4. Fugues de informació	**APLICA**	No existeix cap control específic, però el contracte de confidencialitat ho prohibeix.
12.5.5. Externalització del desenvolupament de programari	**NO APLICA**	No s'externalitza el desenvolupament de programari.
12.6. Gestió de la vulnerabilitat tècnica		
12.6.1. Control de les vulnerabilitats tècniques	**APLICA**	Existeix un registre de vulnerabilitats detectades, que hauria de ser revisat.
13. Gestió de incidents de seguretat de la informació		
13.1. Notificació d'esdeveniments i punts dèbils de seguretat de la informació		
13.1.1. Notificació d'esdeveniments de seguretat de la informació	**APLICA**	Es registren els esdeveniments i es documenten les solucions.
13.1.2. Notificació de punts dèbils de seguretat	**APLICA**	Es documenten i s'intenten millorar o reforçar els punts dèbils del sistema.
13.2. Gestió de incidents de seguretat de la informació i millores		
13.2.1. Responsabilitats i procediments	**APLICA**	Existeix un document que especifica les responsabilitats.
13.2.2. Aprenentatge dels incidents de seguretat de la informació	**APLICA**	Els incidents després de ser solucionats es documenten per futures consultes.
13.2.3. Recopilació d'evidències	**APLICA**	Les evidències es documenten i s'arxiven.
14. Gestió de la continuïtat del negoci		
14.1. Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci		
14.1.1. Inclusió de la seguretat	**APLICA**	No s'ha especificat un pla de

de la informació en el procés de gestió de la continuïtat del negoci		continuïtat del negoci.
14.1.2. Continuïtat del negoci i avaluació de riscs	**APLICA**	No s'ha especificat un pla de continuïtat del negoci.
14.1.3. Desenvolupament i implantació de plans de continuïtat que incloguin la seguretat de la informació	**APLICA**	No s'ha especificat un pla de continuïtat del negoci.
14.1.4. Marc de referència per la planificació de la continuïtat del negoci	**APLICA**	No s'ha especificat un pla de continuïtat del negoci.
14.1.5. Proves, manteniment i re-avaluació dels plans de continuïtat del negoci	**APLICA**	No s'ha especificat un pla de continuïtat del negoci.
15. Compliment		
15.1. Compliment dels requisits legals		
15.1.1. Identificació de la legislació aplicable	**APLICA**	La legislació aplicable esta documentada i es té en compte.
15.1.2. Drets de propietat intel·lectual (IPR)	**APLICA**	Els drets de propietat intel·lectual estan perfectament definits.
15.1.3. Protecció dels documents de l'organització	**APLICA**	Els documents de l'empresa estan protegits legalment.
15.1.4. Protecció de dades i privacitat de la informació de caràcter personal	**APLICA**	L'empresa té un seguiment de la LOPDP, en el que fa referència a les dades de caràcter personal.
15.1.5. Prevenció d'ús indegut dels recursos de tractament de la informació	**APLICA**	El marc legal de l'empresa indica les conseqüències de l'ús indegut dels recursos.
15.1.6. Regulació dels controls criptogràfics	**APLICA**	No està especificat.
15.2. Compliment de les polítiques i normes de seguretat i compliment tècnic		
15.2.1. Compliment de les polítiques i normes de seguretat	**APLICA**	En l'actualitat encara no s'ha realitzat una auditoria que ens permeti saber el compliment de les polítiques i normes de seguretat.
15.2.2. Comprovació del compliment tècnic	**APLICA**	No s'ha realitzat una comprovació del compliment tècnic.
15.3. Consideracions sobre la auditoria dels sistemes de informació		
15.3.1. Controls d'auditoria dels sistemes de informació	**APLICA**	No s'ha realitzat fins a l'actualitat controls d'auditoria dels sistemes d'informació.
15.3.2. Protecció de les eines d'auditoria dels sistemes de informació	**APLICA**	No s'ha especificat la protecció de les eines d'auditoria dels sistemes d'informació.

2.8. Resultats de la Fase II:

En aquesta fase s'han pogut observar els principals documents que ha de disposar la nostre organització, com és la política de seguretat que tots els integrants de l'organització han de complir i utilitzar diàriament. Així mateix, també s'ha especificat el procediment a seguir en les auditories internes, la gestió d'indicadors, el procediment de revisió per direcció, així com la metodologia a seguir al realitzar el posterior anàlisi de riscos, i la declaració d'aplicabilitat, per conèixer quins elements de la ISO 27002 són aplicables en la nostre organització. Un cop ja hem especificat tots aquests elements podem procedir a realitzar l'anàlisi de riscos de la següent fase, tenint clar que ja s'han especificat els paràmetres necessaris per saber els procediments i normatives a seguir per tota l'organització.

Un punt important a destacar en aquest apartat és que perquè aquestes normatives siguin conegudes i respectades per tota l'organització s'haurà de programar un conjunt de sessions de formació pels diferents membres implicats.

Per resumir-ho en uns punts, podem dir:

- S'han pogut crear els principals documents que ha de disposar qualsevol organització i que s'han comentat anteriorment.

- S'ha revisat la documentació perquè sigui fàcil de comprendre pels usuaris del sistema i per tant, augmenti el compliment de la mateixa.

- S'ha fomentat la divulgació de la documentació segons els perfils, en cursos de formació (projecte de la fase IV).

- S'han pogut conèixer amb la declaració d'aplicabilitat quins elements de la normativa ISO són aplicables en la nostre organització.

- S'ha fomentat que en un futur aquestes documentacions es revisin periòdicament i és vagin millorant amb les novetats i actualitzacions necessàries.

3. FASE III – Anàlisis de riscos:

3.1. Introducció:

En la realització d'un anàlisi de riscos podrem identificar els diferents riscos a que està exposada la nostre empresa o organització, i ens permetrà determinar de manera més precisa quines mesures de seguretat seran les més idònies per les nostres instal·lacions, i pels diferents actius identificats de l'empresa. A més ens permetrà identificar el risc residual i el risc real que està exposada la nostre empresa.

En els següents apartats podrem observar, l'inventari dels diferents actius de la nostre organització, i les diferents amenaces a que està exposada aquesta empresa. Per tant, al finalitzar obtindrem un complet anàlisi de riscos de l'empresa.

3.2. Inventari d'actius:

És important realitzar un anàlisi detallat dels actius seguint la metodologia MAGERIT. Podem dir també que els "actius" són bens de l'organització o empresa, que es troben relacionats amb l'activitat de l'empresa, ja siguin programaris, maquinari, o qualsevol equipament de les instal·lacions principals o auxiliars, o les xarxes del sistema de dades, entre d'altres. En el present apartat ens centrarem en els elements següents:

- Instal·lacions
- Maquinari
- Aplicacions
- Dades
- Xarxes
- Serveis
- Equipament auxiliar
- Personal

Cal destacar que degut a que a l'empresa existeixen alguns actius d'idèntiques característiques, en el següents taules s'agruparan els actius repetits.

Inventari agrupat dels actius de instal·lacions:

Àmbit	ID	Actiu
Instal·lacions	[I.1]	Centre de Processament de Dades de l'empresa (CPD).
	[I.2]	Oficina tècnica del departament TIC.
	[I.3]	Sala del generador elèctric i sistema UPS.
	[I.4]	Resta dependències de l'edifici.

Inventari agrupat dels actius de maquinari:

Àmbit	ID	Actiu
Maquinari	[M.1] [M.2] [M.3]	Servidors: HP ProLiant ML350e Gen8 • Servidor web i d'aplicació mòbil. • Servidor correu electrònic i missatgeria. • Servidor firewall i seguretat.

	[M.4] [M.5] [M.6]	• Servidor bases de dades. • Servidor de còpies de seguretat (backup). • Servidor de proves de desenvolupament.
	[M.7]	Ordinadors de sobretaula: HP Compaq Pro 6300 All-In-One.
	[M.8]	Ordinadors portàtils dels empleats: Ultrabook ASUS 15,6" 856CM Intel Core i5 3317U.
	[M.9]	Smartphones: Samsung Galaxy S3 i S4.
	[M.10]	Switchs de comunicacions de la xarxa, marca Cisco.
	[M.11]	Routers de comunicacions de la xarxa, marca Cisco.
	[M.12]	Sistemes de backup NAS.
	[M.13]	Suports extraïbles (disc durs, usb's).
	[M.14]	Impressores departamentals: HP LaserJet Enterprise 700 MFP M725dn.
	[M.15]	Projectors departamentals: Toshiba TDPP8EU.
	[M.16]	Escàners departamentals: HP Scanjet Enterprise 8500 fn1.
	[M.17]	Pissarres Digitals Sala de Reunió: Smart Board SB680.
	[M.18]	Replicador de senyal wifi Allied Telesis per augmentar cobertura a interior empresa.

Inventari agrupat dels actius d'aplicacions:

Àmbit	ID	Actiu
Aplicacions	[A.1]	Sistemes operatius servidors: • Microsoft Windows Server 2012. • Linux Ubuntu Server.
	[A.2]	Sistemes operatius personals: • Microsoft Windows 7. • Linux Ubuntu 13.04.
	[A.3]	Sistema operatiu smartphones: • Android 4.2 JellyBean.
	[A.4]	Gestor Documental Oracle WebCenter.
	[A.5]	Sistema de monitorització Snort.
	[A.6]	Sistema Apache y Mysql, Xampp/Lamp.
	[A.7]	Desenvolupaments Eclipse IDE.
	[A.8]	Antivirus: McAfee SaaS Total Protection (PC, servidors, correu electrònic i web).
	[A.9]	Sistema de còpies de seguretat.
	[A.10]	Aplicació mòbil empresa.
	[A.11]	Portal web empresa.
	[A.12]	Suite ofimàtica Microsoft Office Professional 2013.

Inventari agrupat dels actius de dades:

Àmbit	ID	Actiu
Dades	[D.1]	Base de dades de clients registrats.
	[D.2]	Base de dades d'empleats de l'empresa.
	[D.3]	Base de dades del gestor documental per aplicació mòbil i portal web de propietats immobiliàries, poblacions, fotografies i vídeos, anuncis, i documentació relacionada.

	[D.4]	Base de dades proveïdors i facturació.
	[D.5]	Codi font dels desenvolupaments.
	[D.6]	Gestor documental empresa amb documentació dels sistema i dels diferents departaments de l'empresa.
	[D.7]	Registres de log i alertes.

Inventari agrupat dels actius de xarxes:

Àmbit	ID	Actiu
Xarxes	[X.1]	Xarxa interna ethernet local.
	[X.2]	Xarxa de fibra òptica externa.
	[X.3]	Xarxa de telefonia fixa.

Inventari agrupat dels actius de serveis:

Àmbit	ID	Actiu
Serveis	[S.1]	Servei d'Internet extern.
	[S.2]	Servei d'Intranet local.
	[S.3]	Correu electrònic i missatgeria.
	[S.4]	Telefonia fixa.
	[S.5]	Consulta i modificació dades del gestor documental.
	[S.6]	Consulta i modificació de dades de les bases de dades.
	[S.7]	Consulta portal web i aplicació mòbil.

Inventari agrupat dels actius d'equipament auxiliar:

Àmbit	ID	Actiu
Equipament auxiliar	[EA.1]	Sistema SAI / UPS: SAI Salicru SPS ADVANCE.
	[EA.2]	Generador elèctric.
	[EA.3]	Aire condicionat: Daikin.
	[EA.4]	Sensors de temperatura, humitat i moviment.
	[EA.5]	Cablejat elèctric general.
	[EA.6]	Cablejat de dades ethernet: cables UTP CAT6.
	[EA.7]	Armaris de protecció.

Inventari agrupat dels actius de personal:

Àmbit	ID	Actiu
Personal	[P.1]	Director General.
	[P.2]	Director de Comptabilitat i Finances.
	[P.3]	Director de Màrqueting.
	[P.4]	Director TIC.
	[P.5]	Director Atenció Usuari.
	[P.6]	Director de RRHH.
	[P.7]	Director de Desenvolupaments.
	[P.8]	Administratives Comptabilitat i Finances.
	[P.9]	Comercials.
	[P.10]	Administradors TIC.
	[P.11]	Tècnics Atenció Usuari.

	[P.12]	Tècnic de RRHH.
	[P.13]	Desenvolupadors.
	[P.14]	Proveïdors.
	[P.15]	Personal de recepció i seguretat.
	[P.16]	Usuaris del sistema.

Dependències entre actius:

El concepte de "dependència entre actius", és basa que davant un incident de seguretat de quina manera un actiu superior depèn d'un actiu inferior, per tant, quan es produeix l'incident en l'actiu inferior quin perjudici té per un actiu superior.

Una forma de no sobrecarregar les taules i no realitzar dependències cícliques entre els diferents elements, podem suposar el següent nivell de dependències:

- Instal·lacions: dependrà de:
  - Maquinari
  - Equipament auxiliar
  - Xarxes
  - Personal
- Maquinari: dependrà de:
  - Instal·lacions
  - Aplicacions
  - Dades
  - Xarxes
  - Serveis
  - Equipament auxiliar
  - Personal
- Aplicacions: dependrà de:
  - Maquinari
  - Serveis
  - Xarxes
  - Personal
- Dades: dependrà de:
  - Maquinari
  - Aplicacions
  - Serveis
  - Personal
- Xarxes: dependrà de:
  - Maquinari
  - Instal·lacions
  - Serveis
  - Equipament auxiliar
  - Personal
- Serveis: dependrà de:
  - Aplicacions
  - Maquinari
  - Xarxes
  - Personal
- Equipament auxiliar: dependrà de:

- ❖ Maquinari
- ❖ Instal·lacions
- ❖ Personal

- Personal: dependrà de:
  - ❖ Segons organigrama de l'empresa

3.3. Valoració d'actius:

També serà molt important el punt de valorar els nostres actius segons la metodologia MAGERIT, amb l'estimació quantitativa, tenint en compte paràmetres com podrien ser el que ens costaria la seva reposició, l'ús que se'n fa, la repercussió que pot tenir, el temps a reposar-lo, entre d'altres, i un cop obtinguts aquests paràmetres per part dels empleats de l'empresa, podrem realitzar-ne una abstracció en 5 nivells, tal com podem veure tot seguit en les següents categories:

Valoració	Rang	Valor en €
Molt alt (MA)	valor >=200.000€	300.000€
Alt (A)	100.00€< valor <= 200.000€	150.000€
Mitja (M)	50.00€< valor <= 100.000€	75.000€
Baix (B)	10.000€<valor<=50.000€	30.000€
Molt Baix (MB)	Valor<=10.000€	10.000€

3.4. Dimensions de seguretat:

En aquest apartat, un cop identificats els actius, els valorarem segons la criticitat a les cinc dimensions de la seguretat de la informació (ACIDT), i per tant, ens permetrà valorar l'impacte de la materialització d'una amenaça sobre un actiu exposat.

Podem trobar les següents dimensions de seguretat, que tot seguit utilitzarem:

- Autenticitat i no-repudi [A]: Ens permet assegurar la identitat dels recursos, documents, usuaris o processos del sistema d'informació.

- Confidencialitat [C]: Ens permet assegurar que només els usuaris autoritzats poden tenir accés a la informació dels diferents nivells de seguretat.

- Integritat [I]: Ens permet assegurar que la informació és completa i exacta, i que no ha estat manipulada per usuaris no autoritzats.

- Disponibilitat [D]: Ens permet assegurar que els sistemes, processos i informació estarà disponible pels usuaris autoritzats en el moment que sigui precís.

- Traçabilitat [T]: Ens permet seguir el recorregut històric d'un procés, document o informació concreta, determinant precisament quin usuari ha realitzat cadascuna de les accions.

El valor que rebrà l'actiu podrà ser propi o acumulat. El valor propi s'assignarà a la informació, quedant la resta d'actius subordinats a les necessitats d'explotació i protecció de la informació. D'aquesta manera, els actius inferiors en un esquema de

dependències acumulen el valor dels actius que es recolzen en ells. Cada actiu de informació pot tenir un valor diferent a cadascuna de les diferents dimensions per a la organització que desitgem analitzar.

Valor	Criteri
10	Dany molt greu a l'organització.
7 a 9	Dany greu a l'organització.
4 a 6	Dany important a l'organització.
1 a 3	Dany menor a l'organització.
0	Dany irrellevant a l'organització.

3.5. Taula resum de la valoració:

Tot seguit podem veure una taula on reflectir les valoracions dels actius, i els seus aspectes crítics:

ID	Actiu	Valor	Depèn	Aspectes crítics				
Instal·lacions				**A**	**C**	**I**	**D**	**T**
[I.1]	CPD empresa.	MA	[M] [X] [EA] [P]	10	10	10	10	10
[I.2]	Oficina tècnica del departament TIC.	A		x	8	x	8	8
[I.3]	Sala del generador elèctric i sistema UPS.	A		x	8	x	8	8
[I.4]	Resta dependències de l'edifici.	MA		x	6	x	8	8
Maquinari				**A**	**C**	**I**	**D**	**T**
[M.1]	Servidors: HP ProLiant ML350e Gen8 • Servidor web i d'aplicació mòbil.	M	[I] [X] [A] [S] [D] [EA] [P]	9	8	8	9	9
[M.2]	Servidors: HP ProLiant ML350e Gen8 • Servidor correu electrònic i missatgeria.	M		9	8	8	9	9
[M.3]	Servidors: HP ProLiant ML350e Gen8 • Servidor Firewall i seguretat.	M		9	9	8	9	9
[M.4]	Servidors: HP ProLiant ML350e Gen8 • Servidor bases de dades.	M		9	9	8	9	9
[M.5]	Servidors: HP ProLiant ML350e Gen8 • Servidor de còpies de seguretat.	M		9	9	8	9	9
[M.6]	Servidors: HP ProLiant ML350e Gen8 • Servidor de proves de desenvolupament.	M		9	10	8	8	9

[M.7]	Ordinadors de sobretaula: HP Compaq Pro 6300 All-In-One.	M		8	7	8	8	9
[M.8]	Ordinadors portàtils: Ultrabook ASUS 15,6" 856CM Intel Core i5 3317U.	M		8	7	8	7	9
[M.9]	Smartphones: Samsung Galaxy S3 i S4.	MB		8	7	8	7	9
[M.10]	Switchs de comunicacions, Cisco.	MB		8	8	8	8	9
[M.11]	Routers de comunicacions, Cisco.	MB		8	8	8	8	9
[M.12]	Sistemes NAS.	A		9	9	9	9	9
[M.13]	Suports extraïbles.	MB		8	8	8	7	9
[M.14]	Impressores: HP Laser Jet Enterprise 700 MFP M725dn.	MB		5	5	7	6	6
[M.15]	Projectors: Toshiba TDPP8EU.	MB		5	5	7	6	6
[M.16]	Escàners: HP Scanjet Enterprise 8500 fn1.	MB		5	5	7	6	6
[M.17]	Pissarres Digitals: Smart Board SB680.	MB		5	5	7	6	6
[M.18]	Replicador de senyal wifi Allied Telesis.	MB		9	9	9	7	9
Aplicacions				**A**	**C**	**I**	**D**	**T**
[A.1]	Sistemes operatius servidors.	M		8	8	8	9	9
[A.2]	Sistemes operatius personals.	B		8	8	8	7	8
[A.3]	Sistema operatiu smartphones.	MB		8	8	8	6	8
[A.4]	Gestor Documental Oracle WebCenter.	M		8	9	9	8	9
[A.5]	Sistema de monitorització Snort.	MB	[M]	8	9	9	9	8
[A.6]	Sistema Apache y Mysql, Xampp/Lamp.	B	[S]	8	9	9	9	9
[A.7]	Desenvolupaments Eclipse IDE.	MB	[X]	8	9	8	7	9
[A.8]	Antivirus: McAfee SaaS Total Protection.	B	[P]	8	9	8	9	8
[A.9]	Sistema de còpies de seguretat.	M		8	9	9	9	9
[A.10]	Aplicació mòbil empresa.	A		9	8	9	9	8
[A.11]	Portal web empresa.	A		9	8	9	9	8
[A.12]	Suite Ofimàtica Microsoft Office Professional 2013.	B		5	5	7	7	6
Dades				**A**	**C**	**I**	**D**	**T**
[D.1]	BBDD clients registrats.	MA		9	9	9	8	9
[D.2]	BBDD d'empleats.	MA	[M]	9	9	9	8	9
[D.3]	BBDD del gestor documental per aplicació mòbil i portal web.	MA	[A]	9	9	9	8	9
[D.4]	BBDD proveïdors i facturació.	MA		9	9	9	8	9
[D.5]	Codi font dels desenvolupaments.	MA	[S]	9	9	9	8	9
[D.6]	Gestor documental departaments empresa.	MA	[P]	9	8	9	8	9
[D.7]	Registres de log i alertes.	B		8	7	9	8	8
Xarxes				**A**	**C**	**I**	**D**	**T**
[X.1]	Xarxa interna ethernet local.	M	[I] M]	7	7	8	8	8

[X.2]	Xarxa de fibra òptica externa.	M	[P] S]	7	7	8	9	8
[X.3]	Xarxa de telefonia fixa.	B	[EA]	6	6	8	6	7
Serveis				**A**	**C**	**I**	**D**	**T**
[S.1]	Servei d'Internet extern.	MA	[A] [M] [P] [X]	7	7	8	8	8
[S.2]	Servei d'Intranet local.	MA		8	8	8	8	8
[S.3]	Correu electrònic i missatgeria.	M		8	8	8	8	9
[S.4]	Telefonia fixa.	B		6	6	8	6	7
[S.5]	Consulta i modificació dades del gestor documental.	A		8	8	9	8	8
[S.6]	Consulta i modificació de dades de les bases de dades.	A		8	8	9	8	8
[S.7]	Consulta portal web i aplicació mòbil.	MA		8	8	9	8	8
Equipament auxiliar				**A**	**C**	**I**	**D**	**T**
[EA.1]	SAI / UPS: SAI Salicru SPS ADVANCE.	M	[I] [P]	x	6	x	8	x
[EA.2]	Generador elèctric.	MA		x	5	x	8	x
[EA.3]	Aire condicionat: Daikin.	MA		x	5	x	8	x
[EA.4]	Sensors de temperatura, humitat i moviment.	MA		x	5	x	8	x
[EA.5]	Cablejat elèctric general.	A		5	5	x	8	x
[EA.6]	Cablejat de dades ethernet: UTP CAT6.	MA		5	8	x	8	x
[EA.7]	Armaris de protecció.	M		x	6	x	8	x
Personal				**A**	**C**	**I**	**D**	**T**
[P.1]	Director General.	M	x	x	x	x	8	x
[P.2]	Director de Comptabilitat i Finances.	M	[P.1]	x	x	x	7	x
[P.3]	Director de Màrqueting.	M	[P.1]	x	x	x	7	x
[P.4]	Director TIC.	M	[P.1]	x	x	x	9	x
[P.5]	Director Atenció Usuari.	M	[P.1]	x	x	x	8	x
[P.6]	Director de RRHH.	M	[P.1]	x	x	x	7	x
[P.7]	Director de Desenvolupaments.	M	[P.1]	x	x	x	8	x
[P.8]	Administratives Comptabilitat i Finances.	M	[P.2]	x	x	x	7	x
[P.9]	Comercials.	M	[P.3]	x	x	x	6	x
[P.10]	Administradors TIC.	M	[P.4]	x	x	x	9	x
[P.11]	Tècnics Atenció Usuari.	M	[P.5]	x	x	x	9	x
[P.12]	Tècnic de RRHH.	M	[P.6]	x	x	x	6	x
[P.13]	Desenvolupadors.	M	[P.7]	x	x	x	8	x
[P.14]	Proveïdors.	M	[P.2]	x	x	x	9	x
[P.15]	Personal de recepció i seguretat .	M	[P.1]	x	x	x	9	x
[P.16]	Usuaris del sistema.	M	x	x	x	x	9	x

3.6. Anàlisi d'amenaces:

En els diferents actius podrem trobar diferents amenaces de seguretat a les que estan exposats. I posteriorment estimarem la vulnerabilitat de cada actiu respecte les amenaces potencials i la seva freqüència estimada.

Les amenaces, segons el llibre de la metodologia MAGERIT, poden ser d'aquest tipus:

- Desastres naturals.
- Origen industrial.
- Errors i fallades no intencionals.
- Atacs intencionals.

Per a poder determinar la freqüència amb la que és pot materialitzar una amenaça, utilitzarem la següent taula de valors:

Valoració	Valor	Observació
Freqüència molt alta (FA).	**100**	Diàriament.
Freqüent mitjana (FM).	**10**	Mensualment.
Freqüència normal (FN).	**1**	Anualment.
Poca freqüència (PF).	**1/10 (0,1)**	Cada diversos anys.
Molt poca freqüència (MPF).	**1/100 (0,01)**	Casi mai es dona.

Valoració	Impacte %
100%	Molt alt – MA.
75%	Alt – A.
50%	Mitjà – M.
20%	Baix – B.
5%	Molt baix – MB.

La informació que recopilem donarà lloc a una taula de resum, dels diferents actius, i la freqüència de materialització de les diferents amenaces, i el seu impacte a les diferents dimensions de l'actiu.

ID	Actiu	Freqüència	Aspectes crítics				
			A	**C**	**I**	**D**	**T**
Instal·lacions							
[I.1]	CPD empresa.	10	x	x	x	100%	x
[I.2]	Oficina tècnica del departament TIC.	10	x	x	x	100%	x
[I.3]	Sala del generador elèctric i sistema UPS.	10	x	x	x	100%	x
[I.4]	Resta dependències de l'edifici.	10	x	x	x	100%	x
Amenaces							
[N.1]	Foc.	1/100 (0,01)	x	x	x	100%	x
[N.2]	Danys per aigua.	1/100 (0,01)	x	x	x	100%	x
[I.1]	Foc.	1/10 (0,1)	x	x	x	100%	x
[I.2]	Danys per aigua.	1/10 (0,1)	x	x	x	100%	x
[A.7]	Ús no previst.	1	x	x	x	50%	x
[A.11]	Accés no autoritzat.	10	x	x	x	50%	x
[A.26]	Atac destructiu.	1/100 (0,01)	x	x	x	75%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Maquinari (Servidors)							
[M.1]	Servidors: HP ProLiant ML350e Gen8 • Servidor web i d'aplicació mòbil.	10	x	100%	75%	100%	x
[M.2]	Servidors: HP ProLiant ML350e Gen8 • Servidor correu electrònic i missatgeria.	10	x	100%	75%	100%	x
[M.3]	Servidors: HP ProLiant ML350e Gen8 • Servidor Firewall i seguretat.	10	x	100%	75%	100%	x
[M.4]	Servidors: HP ProLiant ML350e Gen8 • Servidor bases de dades.	10	x	100%	75%	100%	x
[M.5]	Servidors: HP ProLiant ML350e Gen8 • Servidor de còpies de seguretat.	10	x	100%	75%	100%	x
[M.6]	Servidors: HP ProLiant ML350e Gen8 • Servidor de proves de desenvolupament.	10	x	100%	75%	100%	x
Amenaces							
[N.1]	Foc.	1/100 (0,01)	x	x	x	100%	x
[N.2]	Danys per aigua.	1/100 (0,01)	x	x	x	100%	x
[I.1]	Foc.	1	x	x	x	100%	x
[I.2]	Danys per aigua.	1/10 (0,1)	x	x	x	100%	x
[I.4]	Contaminació electromagnètica.	1	x	x	x	100%	x
[I.5]	Averia d'origen físic o lògic.	1	x	x	x	100%	x
[I.6]	Tall de subministrament elèctric.	10	x	x	x	100%	x
[I.7]	Condicions inadequades de temperatura i humitat.	10	x	x	x	100%	x
[E.2]	Errors de l'administrador.	10	x	50%	50%	50%	x
[E.23]	Errors de manteniment /actualització d'equips.	10	x	x	x	50%	x
[E.24]	Caiguda del sistema per esgotament de recursos.	10	x	x	x	75%	x
[E.25]	Pèrdua d'equips.	10	x	50%	x	50%	x
[A.6]	Abús de privilegi d'accés.	10	x	70%	75%	75%	x
[A.7]	Ús no previst.	10	x	75%	75%	75%	x
[A.11]	Accés no autoritzat.	10	x	75%	x	75%	x
[A.23]	Manipulació d'equips.	10	x	75%	x	75%	x
[A.24]	Denegació de servei.	1	x	x	x	100%	x
[A.25]	Robatori.	1	x	100%	x	100%	x
[A.26]	Atac destructiu.	1	x	x	x	100%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Maquinari (Equips empleats)							
[M.7]	Ordinadors de sobretaula: HP Compaq Pro 6300 All-In-One.	10	x	75%	50%	100%	x
[M.8]	Ordinadors portàtils: Ultrabook ASUS 15,6" 856CM Intel Core i5 3317U.	10	x	75%	50%	100%	x
[M.9]	Smartphones: Samsung Galaxy S3 i S4.	10	x	75%	50%	100%	x
[M.12]	Sistemes NAS.	10	x	75%	50%	100%	x
[M.13]	Suports extraïbles.	10	x	75%	50%	100%	x
[M.14]	Impressores: HP Laser Jet Enterprise 700 MFP M725dn.	10	x	75%	50%	100%	x
[M.15]	Projectors: Toshiba TDPP8EU.	10	x	75%	50%	100%	x
[M.16]	Escàners: HP Scanjet Enterprise 8500 fn1.	10	x	75%	50%	100%	x
[M.17]	Pissarres Digitals: Smart Board SB680.	10	x	75%	50%	100%	x
Amenaces							
[N.1]	Foc.	1/100 (0,01)	x	x	x	100%	x
[N.2]	Danys per aigua.	1/100 (0,01)	x	x	x	100%	x
[I.1]	Foc.	1/10 (0,1)	x	x	x	100%	x
[I.2]	Danys per aigua.	1/10 (0,1)	x	x	x	100%	x
[I.4]	Contaminació electromagnètica.	1/10 (0,1)	x	x	x	100%	x
[I.5]	Averia d'origen físic o lògic.	1/10 (0,1)	x	x	x	100%	x
[I.6]	Tall de subministrament elèctric.	10	x	x	x	75%	x
[I.7]	Condicions inadequades de temperatura i humitat.	1	x	x	x	75%	x
[E.2]	Errors de l'administrador.	1	x	20%	50%	50%	x
[E.23]	Errors de manteniment /actualització d'equips.	10	x	x	x	50%	x
[E.24]	Caiguda del sistema per esgotament de recursos.	1	x	x	x	75%	x
[E.25]	Pèrdua d'equips.	10	x	50%	x	50%	x
[A.6]	Abús de privilegi d'accés.	10	x	50%	50%	75%	x
[A.7]	Ús no previst.	10	x	75%	50%	75%	x
[A.11]	Accés no autoritzat.	10	x	75%	x	75%	x
[A.23]	Manipulació d'equips.	10	x	75%	x	75%	x
[A.24]	Denegació de servei.	1/10 (0,1)	x	x	x	75%	x
[A.25]	Robatori.	1	x	75%	x	75%	x
[A.26]	Atac destructiu.	1/10 (0,1)	x	x	x	75%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Maquinari (Comunicacions)							
[M.10]	Switchs de comunicacions, Cisco.	1	x	75%	50%	100%	x
[M.11]	Routers de comunicacions, Cisco.	1	x	75%	50%	100%	x
[M.18]	Replicador de senyal wifi Allied Telesis.	1	x	75%	50%	100%	x
Amenaces							
[N.1]	Foc.	1/100 (0,01)	x	x	x	100%	x
[N.2]	Danys per aigua.	1/100 (0,01)	x	x	x	100%	x
[I.1]	Foc.	1/10 (0,1)	x	x	x	100%	x
[I.2]	Danys per aigua.	1/10 (0,1)	x	x	x	100%	x
[I.4]	Contaminació electromagnètica.	1/10 (0,1)	x	x	x	100%	x
[I.5]	Averia d'origen físic o lògic.	1/10 (0,1)	x	x	x	100%	x
[I.6]	Tall de subministrament elèctric.	1	x	x	x	75%	x
[I.7]	Condicions inadequades de temperatura i humitat.	1	x	x	x	75%	x
[E.2]	Errors de l'administrador.	1	x	50%	50%	50%	x
[E.23]	Errors de manteniment /actualització d'equips.	1	x	x	x	50%	x
[E.24]	Caiguda del sistema per esgotament de recursos.	1	x	x	x	75%	x
[E.25]	Pèrdua d'equips.	1	x	5%	x	5%	x
[A.6]	Abús de privilegi d'accés.	1	x	50%	50%	50%	x
[A.7]	Ús no previst.	1	x	50%	50%	50%	x
[A.11]	Accés no autoritzat.	1	x	50%	x	50%	x
[A.23]	Manipulació d'equips.	1/10 (0,1)	x	75%	x	75%	x
[A.24]	Denegació de servei.	1/10 (0,1)	x	x	x	75%	x
[A.25]	Robatori.	1/10 (0,1)	x	75%	x	75%	x
[A.26]	Atac destructiu.	1/10 (0,1)	x	x	x	75%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Aplicacions							
[A.1]	Sistemes operatius servidors.	10	50%	75%	75%	75%	x
[A.2]	Sistemes operatius personals.	10	50%	75%	75%	75%	x
[A.3]	Sistema operatiu smartphones.	10	50%	75%	75%	75%	x
[A.4]	Gestor Documental Oracle WebCenter.	10	50%	75%	75%	75%	x
[A.5]	Sistema de monitorització Snort.	10	50%	75%	75%	75%	x
[A.6]	Sistema Apache y Mysql, Xampp/Lamp.	10	50%	75%	75%	75%	x
[A.7]	Desenvolupaments Eclipse IDE.	10	50%	75%	75%	75%	x
[A.8]	Antivirus: McAfee SaaS Total Protection.	10	50%	75%	75%	75%	x
[A.9]	Sistema de còpies de seguretat.	10	50%	75%	75%	75%	x
[A.10]	Aplicació mòbil empresa.	10	50%	75%	75%	75%	x

[A.11]	Portal web empresa.	10	50%	75%	75%	75%	x
[A.12]	Suite Ofimàtica Microsoft Office Professional 2013.	10	50%	75%	75%	75%	x
Amenaces							
[E.1]	Errors dels usuaris.	10	x	20%	20%	20%	x
[E.2]	Errors dels administradors.	10	x	20%	20%	20%	x
[E.4]	Errors de configuració.	1	x	x	20%	x	x
[E.8]	Difusió de programari maligne.	10	x	50%	50%	50%	x
[E.15]	Alteració accidental de la informació.	1	x	x	50%	x	x
[E.18]	Destrucció de informació.	1	x	x	x	75%	x
[E.19]	Fuga d'informació.	1	x	75%	x	x	x
[E.20]	Vulnerabilitat dels programes.	10	x	50%	50%	50%	x
[E.21]	Errors de manteniment/actualització dels programes.	10	x	x	75%	75%	x
[A.5]	Suplantació d'identitat de l'usuari.	1/10 (0,1)	50%	50%	50%	x	x
[A.6]	Abús de privilegis d'accés.	1/10 (0,1)	x	50%	50%	50%	x
[A.7]	Ús no previst.	1	x	20%	20%	20%	x
[A.8]	Difusió de programari maligne.	1	x	75%	75%	75%	x
[A.11]	Accés no autoritzat.	1/10 (0,1)	x	75%	75%	x	x
[A.15]	Modificació deliberada de la informació.	1/10 (0,1)	x	x	75%	x	x
[A.18]	Destrucció de informació.	1/10 (0,1)	x	x	x	75%	x
[A.19]	Divulgació de informació.	1/10 (0,1)	x	50%	x	x	x
[A.22]	Manipulació de programes.	1/10 (0,1)	x	50%	50%	50%	x

ID	**Actiu**	**Freqüència**	**Aspectes crítics**				
			A	**C**	**I**	**D**	**T**
Dades							
[D.1]	BBDD clients registrats.	1	x	75%	75%	75%	x
[D.2]	BBDD d'empleats.	1	x	75%	75%	75%	x
[D.3]	BBDD del gestor documental per aplicació mòbil i portal web.	1	x	75%	75%	75%	x
[D.4]	BBDD proveïdors i facturació.	1	x	75%	75%	75%	x
[D.5]	Codi font dels desenvolupaments.	1	x	75%	75%	75%	x
[D.6]	Gestor documental departaments empresa.	1	x	75%	75%	75%	x
[D.7]	Registres de log i alertes.	1	x	75%	75%	75%	x
Amenaces							
[E.1]	Errors dels usuaris.	1	x	50%	50%	50%	x
[E.2]	Errors dels administradors.	1	x	75%	75%	75%	x
[E.4]	Errors de configuració.	1	x	x	50%	x	x
[E.15]	Alteració accidental de la informació.	1	x	x	50%	x	x
[E.18]	Destrucció de informació.	1	x	x	x	75%	x
[E.19]	Fuga d'informació.	1/10 (0,1)	x	50%	x	x	x
[A.4]	Manipulació de la configuració.	1/10 (0,1)	x	50%	50%	50%	x
[A.5]	Suplantació d'identitat de l'usuari.	1/100 (0,01)	x	75%	75%	75%	x
[A.6]	Abús del privilegi d'accés.	1/100 (0,01)	x	75%	75%	75%	x
[A.11]	Accés no autoritzat.	1/10 (0,1)	x	75%	75%	x	x

[A.15]	Modificació deliberada de la informació.	1/10 (0,1)	x	x	75%	x	x
[A.18]	Destrucció de informació.	1/10 (0,1)	x	x	x	50%	x
[A.19]	Divulgació de informació.	1/10 (0,1)	x	75%	x	x	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Xarxes							
[X.1]	Xarxa interna ethernet local.	1	x	75%	75%	100%	x
[X.2]	Xarxa de fibra òptica externa.	1	x	75%	75%	100%	x
[X.3]	Xarxa de telefonia fixa.	1	x	75%	75%	100%	x
Amenaces							
[I.8]	Fallada del servei de comunicacions.	1	x	x	x	100%	x
[E.2]	Errors dels administradors.	1	x	20%	20%	100%	x
[E.9]	Errors de re-encaminament.	1/10 (0,1)	x	50%	x	x	x
[E.10]	Errors de seqüencia.	1/10 (0,1)	x	x	20%	x	x
[E.14]	Fugues d'informació.	1/10 (0,1)	x	75%	x	x	x
[E.15]	Alteració accidental de la informació.	1	x	x	20%	x	x
[E.19]	Fugues d'informació.	1/10 (0,1)	x	50%	x	x	x
[E.24]	Caiguda dels sistema per esgotament de recursos.	1/10 (0,1)	x	x	x	100%	x
[A.6]	Abús de privilegis d'accés.	1	x	75%	50%	50%	x
[A.7]	Ús no previst.	1	x	50%	50%	50%	x
[A.9]	Re-encaminament de missatges.	1/10 (0,1)	x	20%	x	x	x
[A.10]	Alteració de seqüència.	1/10 (0,1)	x	20%	50%	x	x
[A.11]	Accés no autoritzat.	1/10 (0,1)	x	50%	50%	x	x
[A.12]	Anàlisis de tràfic.	1/10 (0,1)	x	20%	x	x	x
[A.14]	Interceptació d'informació.	1/100 (0,01)	x	50%	x	x	x
[A.15]	Modificació deliberada de la informació.	1/100 (0,01)	x	x	75%	x	x
[A.24]	Denegació de servei.	1/10 (0,1)	x	x	x	100%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Serveis							
[S.1]	Servei d'Internet extern.	1	20%	50%	75%	75%	20%
[S.2]	Servei d'Intranet local.	1	20%	50%	75%	75%	20%
[S.3]	Correu electrònic i missatgeria.	1	20%	50%	75%	75%	20%
[S.4]	Telefonia fixa.	1	20%	50%	75%	75%	20%
[S.5]	Consulta i modificació dades del gestor documental.	1	20%	50%	75%	75%	20%
[S.6]	Consulta i modificació de dades de les bases de dades.	1	20%	50%	75%	75%	20%
[S.7]	Consulta portal web i aplicació mòbil.	1	20%	50%	75%	75%	20%
Amenaces							
[E.1]	Errors dels usuaris.	1	x	20%	20%	5%	x
[E.2]	Errors dels administradors.	1	x	50%	50%	50%	x

[E.15]	Alteració accidental de la informació.	1	x	x	20%	x	x
[E.18]	Destrucció de informació.	1	x	x	x	75%	x
[E.19]	Fuga d'informació.	1/10 (0,1)	x	50%	x	x	x
[A.5]	Suplantació d'identitat de l'usuari.	1/10 (0,1)	20%	20%	20%	x	x
[A.6]	Abús de privilegis d'accés.	1/10 (0,1)	x	5%	20%	20%	x
[A.7]	Ús no previst.	1	x	20%	50%	50%	x
[A.10]	Alteració de seqüència.	1	x	x	20%	x	x
[A.11]	Accés no autoritzat.	1	x	50%	50%	x	x
[A.13]	Repudi.	1/10 (0,1)	x	x	x	x	20%
[A.15]	Modificació deliberada de la informació.	1/100 (0,01)	x	x	75%	x	x
[A.18]	Destrucció de informació.	1/100 (0,01)	x	x	x	50%	x
[A.19]	Divulgació de informació.	1/100 (0,01)	x	50%	x	x	x
[A.24]	Denegació de servei.	1/10 (0,1)	x	x	x	20%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Equipament auxiliar							
[EA.1]	SAI / UPS: SAI Salicru SPS ADVANCE.	1	x	x	x	100%	x
[EA.2]	Generador elèctric.	1	x	x	x	100%	x
[EA.3]	Aire condicionat: Daikin.	1	x	x	x	100%	x
[EA.4]	Sensors de temperatura, humitat i moviment.	1	x	x	x	100%	x
[EA.5]	Cablejat elèctric general.	1	x	x	x	100%	x
[EA.6]	Cablejat de dades ethernet: UTP CAT6.	1	x	x	x	100%	x
[EA.7]	Armaris de protecció.	1	x	x	x	100%	x
Amenaces							
[N.1]	Foc.	1/100 (0,01)	x	x	x	100%	x
[N.2]	Dany per aigua.	1/100 (0,01)	x	x	x	100%	x
[I.1]	Foc.	1/10 (0,1)	x	x	x	100%	x
[I.2]	Dany per aigua.	1/10 (0,1)	x	x	x	100%	x
[I.5]	Averia d'origen físic o lògic.	1	x	x	x	75%	x
[I.6]	Tall de subministrament elèctric.	1	x	x	x	20%	x
[I.7]	Condicions inadequades de temperatura i humitat.	1/10 (0,1)	x	x	x	20%	x
[I.9]	Interrupció d'altres serveis i subministres essencials.	1	x	x	x	20%	x
[E.23]	Errors de manteniment / actualització d'equips.	1	x	x	x	50%	x
[E.25]	Pèrdua d'equips.	1/100 (0,01)	x	x	x	20%	x
[A.7]	Ús no previst.	1	x	x	x	20%	x
[A.11]	Accés no autoritzat.	1	x	x	x	50%	x
[A.23]	Manipulació dels equips.	1	x	x	x	75%	x
[A.25]	Robatori.	1/100 (0,01)	x	x	x	75%	x
[A.26]	Atac destructiu.	1/100 (0,01)	x	x	x	100%	x

ID	Actiu	Freqüència	Aspectes crítics				
			A	C	I	D	T
Personal							
[P.1]	Director General.	10	x	75%	100%	75%	x
[P.2]	Director de Comptabilitat i Finances.	10	x	75%	100%	75%	x
[P.3]	Director de Màrqueting.	10	x	75%	100%	75%	x
[P.4]	Director TIC.	10	x	75%	100%	75%	x
[P.5]	Director Atenció Usuari.	10	x	75%	100%	75%	x
[P.6]	Director de RRHH.	10	x	75%	100%	75%	x
[P.7]	Director de Desenvolupaments.	10	x	75%	100%	75%	x
[P.8]	Administratives Comptabilitat i Finances.	10	x	75%	100%	75%	x
[P.9]	Comercials.	10	x	75%	100%	75%	x
[P.10]	Administradors TIC.	10	x	75%	100%	75%	x
[P.11]	Tècnics Atenció Usuari.	10	x	75%	100%	75%	x
[P.12]	Tècnic de RRHH.	10	x	75%	100%	75%	x
[P.13]	Desenvolupadors.	10	x	75%	100%	75%	x
[P.14]	Proveïdors.	10	x	75%	100%	75%	x
[P.15]	Personal de recepció i seguretat.	10	x	75%	100%	75%	x
[P.16]	Usuaris del sistema.	10	x	75%	100%	75%	x
Amenaces							
[E.7]	Deficiències en l'organització.	10	x	50%	50%	50%	x
[E.19]	Fugues d'informació.	1/10 (0,1)	x	75%	75%	50%	x
[E.28]	In-disponibilitat del personal.	10	x	x	x	50%	x
[A.29]	Extorsió.	1/100 (0,01)	x	75%	100%	75%	x
[A.30]	Enginyeria social.	1	x	50%	50%	50%	x

3.7. Impacte potencial:

En aquest apartat podrem observar l'impacte potencial que podem suposar per la nostre empresa la pròpia materialització de les diferents amenaces que hem detectat en l'apartat anterior, i d'aquesta manera podrem fixar quines seran prioritàries.

Podem calcular el impacte potencial utilitzant aquesta formula:

IP= Valor de l'actiu (per dimensió de seguretat) x Impacte (degradació causada)

I obtindrem la següent taula:

ID	Actiu	Valoració					Impacte					Impacte Potencial				
Instal·lacions		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[I.1]	CPD empresa.	10	10	10	10	10	x	x	x	100%	x	x	x	x	10	x
[I.2]	Oficina tècnica del departament TIC.	x	8	x	8	8	x	x	x	100%	x	x	x	x	8	x
[I.3]	Sala del generador elèctric i sistema UPS.	x	8	x	8	8	x	x	x	100%	x	x	x	x	8	x
[I.4]	Resta dependències de l'edifici.	x	6	x	8	8	x	x	x	100%	x	x	x	x	8	x
Maquinari		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
	Servidors: HP	9	8	8	9	9	x	100%	75%	100%	x	x	8	6	9	x

[M.1]	ProLiant ML350e Gen8 • Servidor web i d'aplicació mòbil															
[M.2]	Servidors: HP ProLiant ML350e Gen8 • Servidor correu electrònic i missatgeria	9	8	8	9	9	x	100%	75%	100%	x	x	8	6	9	x
[M.3]	Servidors: HP ProLiant ML350e Gen8 • Servidor Firewall i seguretat	9	9	8	9	9	x	100%	75%	100%	x	x	9	6	9	x
[M.4]	Servidors: HP ProLiant ML350e Gen8 • Servidor bases de dades	9	9	8	9	9	x	100%	75%	100%	x	x	9	6	9	x
[M.5]	Servidors: HP ProLiant ML350e Gen8 • Servidor de còpies de seguretat	9	9	8	9	9	x	100%	75%	100%	x	x	9	6	9	x
[M.6]	Servidors: HP ProLiant ML350e Gen8 • Servidor de proves de desenvolupament	9	10	8	8	9	x	100%	75%	100%	x	x	10	6	8	x
[M.7]	Ordinadors de sobretaula: HP Compaq Pro 6300 All-In-One.	8	7	8	8	9	x	75%	50%	100%	x	x	5,25	4	8	x
[M.8]	Ordinadors portàtils: Ultrabook ASUS 15,6" 856CM Intel Core i5 3317U.	8	7	8	7	9	x	75%	50%	100%	x	x	5,25	4	7	x
[M.9]	Smartphones: Samsung Galaxy S3 i S4.	8	7	8	7	9	x	75%	50%	100%	x	x	5,25	4	7	x
[M.10]	Switchs de comunicacions, Cisco.	8	8	8	8	9	x	75%	50%	100%	x	x	6	4	8	x
[M.11]	Routers de comunicacions, Cisco.	8	8	8	8	9	x	75%	50%	100%	x	x	6	4	8	x
[M.12]	Sistemes NAS.	9	9	9	9	9	x	75%	50%	100%	x	x	6,75	4,5	9	x
[M.13]	Suports extraïbles.	8	8	8	7	9	x	75%	50%	100%	x	x	6	4	7	x
[M.14]	Impressores: HP Laser Jet Enterprise	5	5	7	6	6	x	75%	50%	100%	x	x	3,75	3,5	6	x

	700 MFP M725dn.															
[M.15]	Projectors: Toshiba TDPP8EU.	5	5	7	6	6	x	75%	50%	100%	x	x	3,75	3,5	6	x
[M.16]	Escàners: HP Scanjet Enterprise 8500 fn1.	5	5	7	6	6	x	75%	50%	100%	x	x	3,75	3,5	6	x
[M.17]	Pissarres Digitals: Smart Board SB680.	5	5	7	6	6	x	75%	50%	100%	x	x	3,75	3,5	6	x
[M.18]	Replicador de senyal wifi Allied Telesis.	9	9	9	7	9	x	75%	50%	100%	x	x	6,75	4,5	7	x
Aplicacions		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[A.1]	Sistemes operatius servidors.	8	8	8	9	9	50%	75%	75%	75%	x	4	6	6	6,75	x
[A.2]	Sistemes operatius personals.	8	8	8	7	8	50%	75%	75%	75%	x	4	6	6	5,25	x
[A.3]	Sistema operatiu smartphones.	8	8	8	6	8	50%	75%	75%	75%	x	4	6	6	4,5	x
[A.4]	Gestor Documental Oracle WebCenter.	8	9	9	8	9	50%	75%	75%	75%	x	4	6,75	6,75	6	x
[A.5]	Sistema de monitorització Snort.	8	9	9	9	8	50%	75%	75%	75%	x	4	6,75	6,75	6,75	x
[A.6]	Sistema Apache y Mysql, Xampp/Lamp.	8	9	9	9	9	50%	75%	75%	75%	x	4	6,75	6,75	6,75	x
[A.7]	Desenvolupaments Eclipse IDE.	8	9	8	7	9	50%	75%	75%	75%	x	4	6,75	6	5,25	x
[A.8]	Antivirus: McAfee SaaS Total Protection.	8	9	8	9	8	50%	75%	75%	75%	x	4	6,75	6	6,75	x
[A.9]	Sistema de còpies de seguretat	8	9	9	9	9	50%	75%	75%	75%	x	4	6,75	6,75	6,75	x
[A.10]	Aplicació mòbil empresa.	9	8	9	9	8	50%	75%	75%	75%	x	4,5	6	6,75	6,75	x
[A.11]	Portal web empresa.	9	8	9	9	8	50%	75%	75%	75%	x	4,5	6	6,75	6,75	x
[A.12]	Suite Ofimàtica Microsoft Office Professional 2013.	5	5	7	7	6	50%	75%	75%	75%	x	2,5	3,75	5,25	5,25	x
Dades		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[D.1]	BBDD clients registrats.	9	9	9	8	9	x	75%	75%	75%	x	x	6,75	6,75	6	x
[D.2]	BBDD d'empleats.	9	9	9	8	9	x	75%	75%	75%	x	x	6,75	6,75	6	x
[D.3]	BBDD del gestor documental per aplicació mòbil i portal web.	9	9	9	8	9	x	75%	75%	75%	x	x	6,75	6,75	6	x
[D.4]	BBDD proveïdors i facturació.	9	9	9	8	9	x	75%	75%	75%	x	x	6,75	6,75	6	x
[D.5]	Codi font dels desenvolupaments.	9	9	9	8	9	x	75%	75%	75%	x	x	6,75	6,75	6	x
[D.6]	Gestor documental departaments empresa.	9	8	9	8	9	x	75%	75%	75%	x	x	6	6,75	6	x
[D.7]	Registres de log i alertes.	8	7	9	8	8	x	75%	75%	75%	x	x	5,25	6,75	6	x
Xarxes		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[X.1]	Xarxa interna ethernet local.	7	7	8	8	8	x	75%	75%	100%	x	x	5,25	6	8	x
[X.2]	Xarxa de fibra òptica externa.	7	7	8	9	8	x	75%	75%	100%	x	x	5,25	6	9	x
[X.3]	Xarxa de telefonia	6	6	8	6	7	x	75%	75%	100%	x	x	4,5	6	6	x

	fixa.															
Serveis		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[S.1]	Servei d'Internet extern.	7	7	8	8	8	20%	50%	75%	75%	20%	1,4	3,5	6	6	1,6
[S.2]	Servei d'Intranet local.	8	8	8	8	8	20%	50%	75%	75%	20%	1,6	4	6	6	1,6
[S.3]	Correu electrònic i missatgeria.	8	8	8	8	9	20%	50%	75%	75%	20%	1,6	4	6	6	1,8
[S.4]	Telefonia fixa.	6	6	8	6	7	20%	50%	75%	75%	20%	1,2	3	6	4,5	1,4
[S.5]	Consulta i modificació dades del gestor documental.	8	8	9	8	8	20%	50%	75%	75%	20%	1,6	4	6,75	6	1,6
[S.6]	Consulta i modificació de dades de les bases de dades.	8	8	9	8	8	20%	50%	75%	75%	20%	1,6	4	6,75	6	1,6
[S.7]	Consulta portal web i aplicació mòbil.	8	8	9	8	8	20%	50%	75%	75%	20%	1,6	4	6,75	6	1,6
Equipament auxiliar		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[EA.1]	SAI / UPS: SAI Salicru SPS ADVANCE.	x	6	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.2]	Generador elèctric.	x	5	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.3]	Aire condicionat: Daikin.	x	5	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.4]	Sensors de temperatura, humitat i moviment.	x	5	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.5]	Cablejat elèctric general.	5	5	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.6]	Cablejat de dades ethernet: UTP CAT6.	5	8	x	8	x	x	x	x	100%	x	x	x	x	8	x
[EA.7]	Armaris de protecció.	x	6	x	8	x	x	x	x	100%	x	x	x	x	8	x
Personal		**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[P.1]	Director General.	x	x	x	8	x	x	75%	100%	75%	x	x	x	x	6	x
[P.2]	Director de Comptabilitat i Finances.	x	x	x	7	x	x	75%	100%	75%	x	x	x	x	5,25	x
[P.3]	Director de Màrqueting.	x	x	x	7	x	x	75%	100%	75%	x	x	x	x	5,25	x
[P.4]	Director TIC.	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x
[P.5]	Director Atenció Usuari.	x	x	x	8	x	x	75%	100%	75%	x	x	x	x	6	x
[P.6]	Director de RRHH.	x	x	x	7	x	x	75%	100%	75%	x	x	x	x	5,25	x
[P.7]	Director de Desenvolupaments.	x	x	x	8	x	x	75%	100%	75%	x	x	x	x	6	x
[P.8]	Administratives Comptabilitat i Finances.	x	x	x	7	x	x	75%	100%	75%	x	x	x	x	5,25	x
[P.9]	Comercials.	x	x	x	6	x	x	75%	100%	75%	x	x	x	x	4,5	x
[P.10]	Administradors TIC.	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x
[P.11]	Tècnics Atenció Usuari.	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x
[P.12]	Tècnic de RRHH.	x	x	x	6	x	x	75%	100%	75%	x	x	x	x	4,5	x
[P.13]	Desenvolupadors.	x	x	x	8	x	x	75%	100%	75%	x	x	x	x	6	x
[P.14]	Proveïdors.	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x
[P.15]	Personal de recepció i seguretat .	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x
[P.16]	Usuaris del sistema.	x	x	x	9	x	x	75%	100%	75%	x	x	x	x	6,75	x

3.8. Nivell de risc acceptable i risc residual:

La nostre organització ha de decidir quin risc pot assumir, o no assumir-lo, i controlar-lo a través de controls, per tant, haurem de decidir quin risc es acceptable per la nostre organització, i quin nivell de risc no és. Tanmateix, el risc que obtenim després d'aplicar els controls de seguretat, l'anomenarem risc residual.

Podem calcular-ho mitjançant la següent formula:

Risc = Impacte Potencial * Freqüència

Seguidament haurem de proposar un límit pel qual l'empresa decidirà assumir el risc, o pel contrari decidirà introduir controls per mitigar-lo. El principal objectiu serà reduir els riscs que superin aquests límit, ja que eliminar tots els riscos és una tasca casi impossible. Per tant, hem de calcular el risc acceptable per l'empresa:

Risc acceptable = Valor de l'actiu * Impacte * Freqüència

- Valor de l'actiu: Els actius els valorarem del 1 al 10, segons si el dany causat és molt elevat o no, amb un valor central acceptable de 5.

- Impacte: Valorarem l'impacte amb un percentatge, en que 100% és un impacte molt alt i un 5% el mínim, amb un valor acceptable de 30%.

- Freqüència: Serà la freqüència d'ocurrència d'una determinada amenaça per l'organització, amb un valor acceptable de 10.

Per tant, seguint aquests paràmetres podem obtenir el risc acceptable per la nostre empresa amb el següent càlcul:

Risc acceptable = 5 * 30% * 10 = 15

Tot seguit podem veure la taula per tots els actius:

ID	Actiu	Freqüència	Impacte Potencial					Risc Acumulat				
Instal·lacions			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[I.1]	CPD empresa.	10	x	x	x	10	x	x	x	x	100	x
[I.2]	Oficina tècnica del departament TIC.	10	x	x	x	8	x	x	x	x	80	x
[I.3]	Sala del generador elèctric i sistema UPS.	10	x	x	x	8	x	x	x	x	80	x
[I.4]	Resta dependències de l'edifici.	10	x	x	x	8	x	x	x	x	80	x
Maquinari			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[M.1]	Servidors: HP ProLiant ML350e Gen8 • Servidor web i d'aplicació mòbil.	10	x	8	6	9	x	x	80	60	90	x
[M.2]	Servidors: HP	10	x	8	6	9	x	x	80	60	90	x

	ProLiant ML350e Gen8 • Servidor correu electrònic i missatgeria.											
[M.3]	Servidors: HP ProLiant ML350e Gen8 • Servidor Firewall i seguretat.	10	x	9	6	9	x	x	90	60	90	x
[M.4]	Servidors: HP ProLiant ML350e Gen8 • Servidor bases de dades.	10	x	9	6	9	x	x	90	60	90	x
[M.5]	Servidors: HP ProLiant ML350e Gen8 • Servidor de còpies de seguretat.	10	x	9	6	9	x	x	90	60	90	x
[M.6]	Servidors: HP ProLiant ML350e Gen8 • Servidor de proves de desenvolupament	10	x	10	6	8	x	x	100	60	80	x
[M.7]	Ordinadors de sobretaula: HP Compaq Pro 6300 All-In-One.	10	x	5,25	4	8	x	x	52,5	40	80	x
[M.8]	Ordinadors portàtils: Ultrabook ASUS 15,6” 856CM Intel Core i5 3317U.	10	x	5,25	4	7	x	x	52,5	40	70	x
[M.9]	Smartphones: Samsung Galaxy S3 i S4.	10	x	5,25	4	7	x	x	52,5	40	70	x
[M.10]	Switchs de comunicacions, Cisco.	1	x	6	4	8	x	x	6	4	8	x
[M.11]	Routers de comunicacions, Cisco.	1	x	6	4	8	x	x	6	4	8	x
[M.12]	Sistemes NAS.	10	x	6,75	4,5	9	x	x	67,5	45	90	x
[M.13]	Suports extraïbles.	10	x	6	4	7	x	x	60	40	70	x
[M.14]	Impressores: HP Laser Jet Enterprise 700 MFP M725dn.	10	x	3,75	3,5	6	x	x	37,5	35	60	x
[M.15]	Projectors: Toshiba TDPP8EU.	10	x	3,75	3,5	6	x	x	37,5	35	60	x
[M.16]	Escàners: HP Scanjet Enterprise 8500 fn1.	10	x	3,75	3,5	6	x	x	37,5	35	60	x
[M.17]	Pissarres Digitals: Smart Board SB680.	10	x	3,75	3,5	6	x	x	37,5	35	60	x

[M.18]	Replicador de senyal wifi Allied Telesis.	1	x	6,75	4,5	7	x	x	6,75	4,5	7	x
Aplicacions			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[A.1]	Sistemes operatius servidors.	10	4	6	6	6,75	x	40	60	60	67,5	x
[A.2]	Sistemes operatius personals.	10	4	6	6	5,25	x	40	60	60	52,5	x
[A.3]	Sistema operatiu smartphones.	10	4	6	6	4,5	x	40	60	60	45	x
[A.4]	Gestor Documental Oracle WebCenter.	10	4	6,75	6,75	6	x	40	67,5	67,5	60	x
[A.5]	Sistema de monitorització Snort.	10	4	6,75	6,75	6,75	x	40	67,5	67,5	67,5	x
[A.6]	Sistema Apache y Mysql, Xampp/Lamp.	10	4	6,75	6,75	6,75	x	40	67,5	67,5	67,5	x
[A.7]	Desenvolupaments Eclipse IDE.	10	4	6,75	6	5,25	x	40	67,5	60	52,5	x
[A.8]	Antivirus: McAfee SaaS Total Protection.	10	4	6,75	6	6,75	x	40	67,5	60	67,5	x
[A.9]	Sistema de còpies de seguretat	10	4	6,75	6,75	6,75	x	40	67,5	67,5	67,5	x
[A.10]	Aplicació mòbil empresa.	10	4,5	6	6,75	6,75	x	45	60	67,5	67,5	x
[A.11]	Portal web empresa.	10	4,5	6	6,75	6,75	x	45	60	67,5	67,5	x
[A.12]	Suite Ofimàtica Microsoft Office Professional 2013.	10	2,5	3,75	5,25	5,25	x	25	37,5	52,5	52,5	x
Dades			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[D.1]	BBDD clients registrats.	1	x	6,75	6,75	6	x	6,75	6,75	6	6,75	x
[D.2]	BBDD d'empleats.	1	x	6,75	6,75	6	x	6,75	6,75	6	6,75	x
[D.3]	BBDD del gestor documental per aplicació mòbil i portal web.	1	x	6,75	6,75	6	x	6,75	6,75	6	6,75	x
[D.4]	BBDD proveïdors i facturació.	1	x	6,75	6,75	6	x	6,75	6,75	6	6,75	x
[D.5]	Codi font dels desenvolupaments.	1	x	6,75	6,75	6	x	6,75	6,75	6	6,75	x
[D.6]	Gestor documental departaments empresa.	1	x	6	6,75	6	x	6	6,75	6	6	x
[D.7]	Registres de log i alertes.	1	x	5,25	6,75	6	x	5,25	6,75	6	5,25	x
Xarxes			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[X.1]	Xarxa interna ethernet local.	1	x	5,25	6	8	x	x	5,25	6	8	x
[X.2]	Xarxa de fibra òptica externa.	1	x	5,25	6	9	x	x	5,25	6	9	x
[X.3]	Xarxa de telefonia fixa.	1	x	4,5	6	6	x	x	4,5	6	6	x
Serveis			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[S.1]	Servei d'Internet extern.	1	1,4	3,5	6	6	1,6	1,4	3,5	6	6	1,6
[S.2]	Servei d'Intranet local.	1	1,6	4	6	6	1,6	1,6	4	6	6	1,6
[S.3]	Correu electrònic i missatgeria.	1	1,6	4	6	6	1,8	1,6	4	6	6	1,8

[S.4]	Telefonia fixa.	1	1,2	3	6	4,5	1,4	1,2	3	6	4,5	1,4
[S.5]	Consulta i modificació dades del gestor documental.	1	1,6	4	6,75	6	1,6	1,6	4	6,75	6	1,6
[S.6]	Consulta i modificació de dades de les bases de dades.	1	1,6	4	6,75	6	1,6	1,6	4	6,75	6	1,6
[S.7]	Consulta portal web i aplicació mòbil.	1	1,6	4	6,75	6	1,6	1,6	4	6,75	6	1,6
Equipament auxiliar			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[EA.1]	SAI / UPS: SAI Salicru SPS ADVANCE.	1	x	x	x	8	x	x	x	x	8	x
[EA.2]	Generador elèctric.	1	x	x	x	8	x	x	x	x	8	x
[EA.3]	Aire condicionat: Daikin.	1	x	x	x	8	x	x	x	x	8	x
[EA.4]	Sensors de temperatura, humitat i moviment.	1	x	x	x	8	x	x	x	x	8	x
[EA.5]	Cablejat elèctric general.	1	x	x	x	8	x	x	x	x	8	x
[EA.6]	Cablejat de dades ethernet: UTP CAT6.	1	x	x	x	8	x	x	x	x	8	x
[EA.7]	Armaris de protecció.	1	x	x	x	8	x	x	x	x	8	x
Personal			**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[P.1]	Director General.	10	x	x	x	6	x	x	x	x	60	x
[P.2]	Director de Comptabilitat i Finances.	10	x	x	x	5,25	x	x	x	x	52,5	x
[P.3]	Director de Màrqueting.	10	x	x	x	5,25	x	x	x	x	52,5	x
[P.4]	Director TIC.	10	x	x	x	6,75	x	x	x	x	67,5	x
[P.5]	Director Atenció Usuari.	10	x	x	x	6	x	x	x	x	60	x
[P.6]	Director de RRHH.	10	x	x	x	5,25	x	x	x	x	52,5	x
[P.7]	Director de Desenvolupaments.	10	x	x	x	6	x	x	x	x	60	x
[P.8]	Administratives Comptabilitat i Finances.	10	x	x	x	5,25	x	x	x	x	52,5	x
[P.9]	Comercials.	10	x	x	x	4,5	x	x	x	x	45	x
[P.10]	Administradors TIC.	10	x	x	x	6,75	x	x	x	x	67,5	x
[P.11]	Tècnics Atenció Usuari.	10	x	x	x	6,75	x	x	x	x	67,5	x
[P.12]	Tècnic de RRHH.	10	x	x	x	4,5	x	x	x	x	45	x
[P.13]	Desenvolupadors.	10	x	x	x	6	x	x	x	x	60	x
[P.14]	Proveïdors.	10	x	x	x	6,75	x	x	x	x	67,5	x
[P.15]	Personal de recepció i seguretat.	10	x	x	x	6,75	x	x	x	x	67,5	x
[P.16]	Usuaris del sistema.	10	x	x	x	6,75	x	x	x	x	67,5	x

3.9. Resultats:

Un cop hem finalitzat aquesta fase disposem d'uns certs elements que ens permeten tenir un anàlisi detallat dels actius rellevants per la seguretat de l'empresa, així mateix s'ha pogut realitzar un estudi de les possibles amenaces dels nostres sistemes

d'informació de l'empresa, i el seu impacte potencial, en el cas que alguna d'aquestes amenaces acabes realitzant-se i produint un problema per la nostre organització.

Hem pogut observar que en molts casos es supera el risc màxim que l'empresa està disposada a acceptar, i que per tant, s'haurà de tractar amb nous projectes que facin augmentar la seguretat de tota la infraestructura i dels actius que s'han marcat com a més problemàtics.

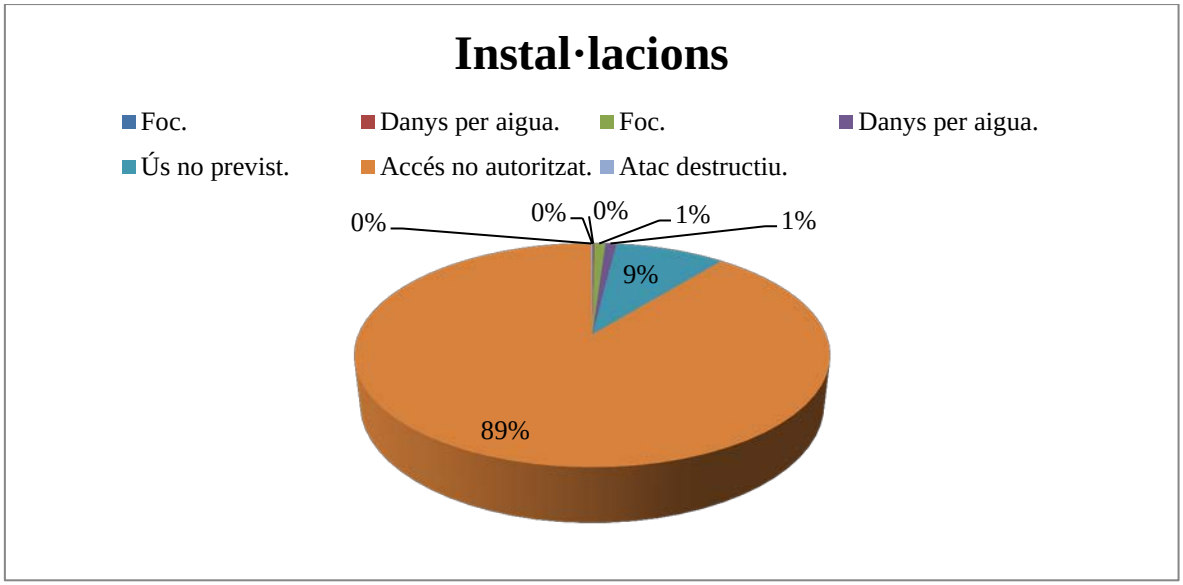
També cal destacar que el risc no serà eliminable al 100%, però podrem minimitzar en alguns casos la materialització de l'amenaça, fent que la gestió dels riscos sigui més gestionable, si s'actualitza degudament i periòdicament.

Seguint aquesta línia, en la següent fase, podrem proposar alguns importants projectes que ens ajudin a minimitzar o controlar les amenaces i per tant, augmentar la seguretat dels nostres sistemes.

A mode de resum es pot dir que:

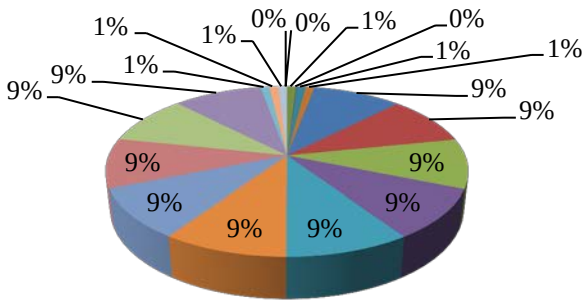
- Disposem d'un anàlisi detallat dels actius de l'organització.
- Disposem d'un anàlisi detallat de les amenaces i riscos de l'empresa.
- Hem pogut observar en quins casos el risc màxim es assumible i en quins casos supera el llindar.
- Sabem amb deteniment en quins casos caldrà crear un nou projecte per millorar la seguretat i rebaixar el risc.
- S'ha pogut concloure que el risc no és eliminable al 100%, sinó que segons el cost l'haurem d'assumir o cedir (assegurances).

Podem veure en els següents gràfics quines amenaces poden tenir més incidència en cada agrupació d'actius:



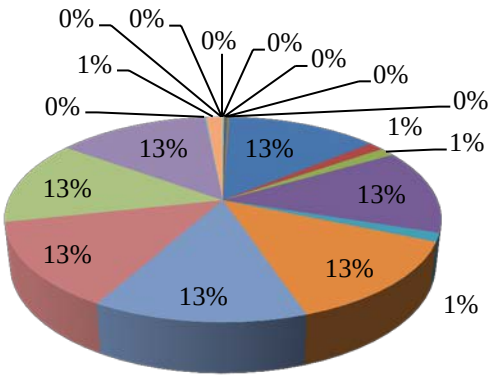
Maquinari (Equips Servidors)

- Foc.
- Foc.
- Contaminació electromagnètica.
- Tall de subministrament elèctric.
- Errors de l'administrador.
- Caiguda del sistema per esgotament de recursos.
- Abús de privilegi d'accés.
- Accés no autoritzat.
- Denegació de servei.
- Atac destructiu.
- Danys per aigua.
- Danys per aigua.
- Averia d'origen físic o lògic.
- Condicions inadequades de temperatura i humitat.
- Errors de manteniment /actualització d'equips.
- Pèrdua d'equips.
- Ús no previst.
- Manipulació d'equips.
- Robatori.



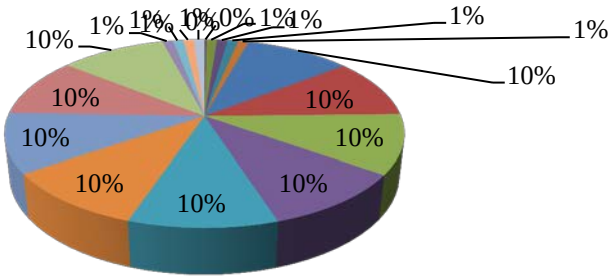
Maquinari (Equips Empleats)

- Foc.
- Foc.
- Contaminació electromagnètica.
- Tall de subministrament elèctric.
- Errors de l'administrador.
- Caiguda del sistema per esgotament de recursos.
- Abús de privilegi d'accés.
- Accés no autoritzat.
- Denegació de servei.
- Atac destructiu.
- Danys per aigua.
- Danys per aigua.
- Averia d'origen físic o lògic.
- Condicions inadequades de temperatura i humitat.
- Errors de manteniment /actualització d'equips.
- Pèrdua d'equips.
- Ús no previst.
- Manipulació d'equips.
- Robatori.



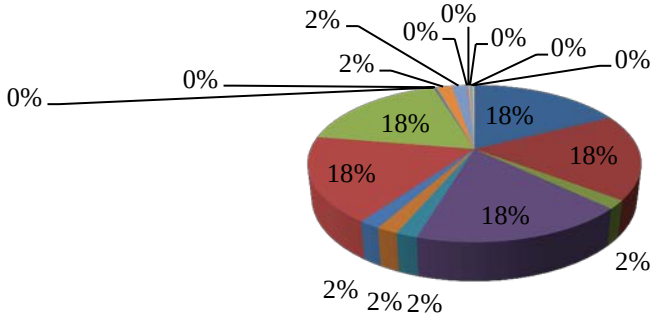
Maquinari (Comunicacions)

- Foc.
- Danys per aigua.
- Foc.
- Danys per aigua.
- Contaminació electromagnètica.
- Averia d'origen físic o lògic.
- Tall de subministrament elèctric.
- Condicions inadequades de temperatura i humitat.
- Errors de l'administrador.
- Errors de manteniment /actualització d'equips.
- Caiguda del sistema per esgotament de recursos.
- Pèrdua d'equips.
- Abús de privilegi d'accés.
- Ús no previst.
- Accés no autoritzat.
- Manipulació d'equips.
- Denegació de servei.
- Robatori.
- Atac destructiu.



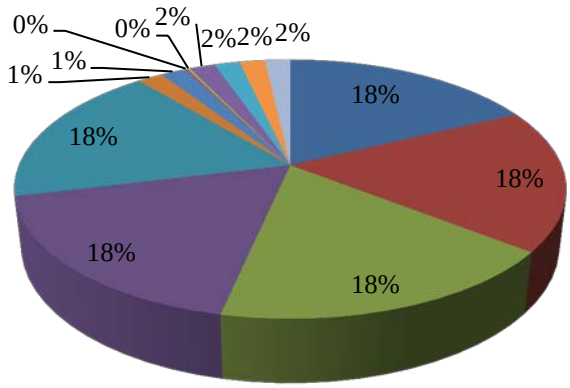
Aplicacions

- Errors dels usuaris.
- Errors dels administradors.
- Errors de configuració.
- Difusió de programari maligne.
- Alteració accidental de la informació.
- Destrucció de informació.
- Fuga d'informació.
- Vulnerabilitat dels programes.
- Errors de manteniment/actualització dels programes.
- Suplantació d'identitat de l'usuari.
- Abús de privilegis d'accés.
- Ús no previst.
- Difusió de programari maligne.
- Accés no autoritzat.
- Modificació deliberada de la informació.
- Destrucció de informació.
- Divulgació de informació.
- Manipulació de programes.



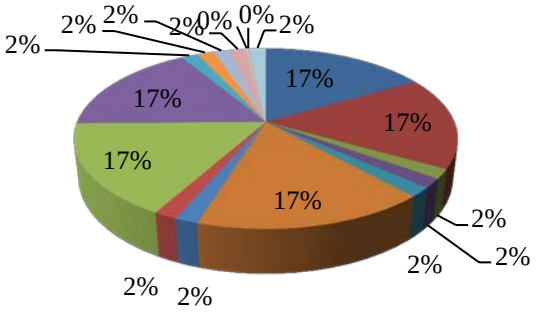
Dades

- Errors dels usuaris.
- Errors dels administradors.
- Errors de configuració.
- Alteració accidental de la informació.
- Destrucció de informació.
- Fuga d'informació.
- Manipulació de la configuració.
- Suplantació d'identitat de l'usuari.
- Abús del privilegi d'accés.
- Accés no autoritzat.
- Modificació deliberada de la informació.
- Destrucció de informació.
- Divulgació de informació.



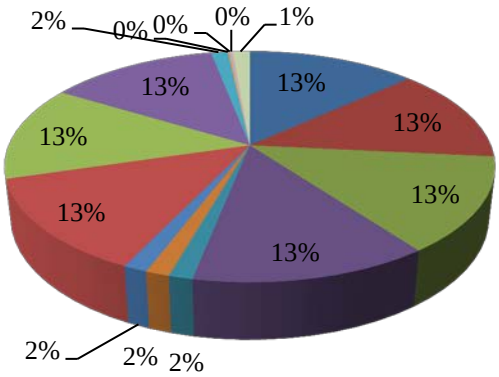
Xarxes

- Fallada del servei de comunicacions.
- Errors dels administradors.
- Errors de re-encaminament.
- Errors de seqüencia.
- Fugues d'informació.
- Alteració accidental de la informació.
- Fugues d'informació.
- Caiguda dels sistema per esgotament de recursos.
- Abús de privilegis d'accés.
- Ús no previst.
- Re-encaminament de missatges.
- Alteració de seqüència.
- Accés no autoritzat.
- Anàlisis de tràfic.
- Interceptació d'informació.
- Modificació deliberada de la informació.
- Denegació de servei.



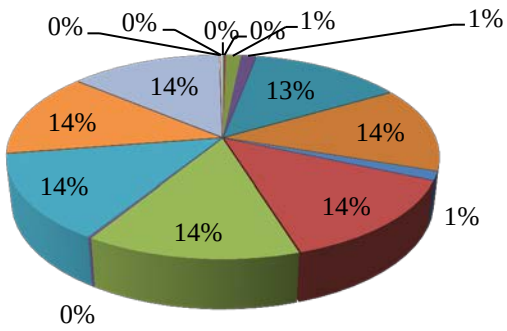
Serveis

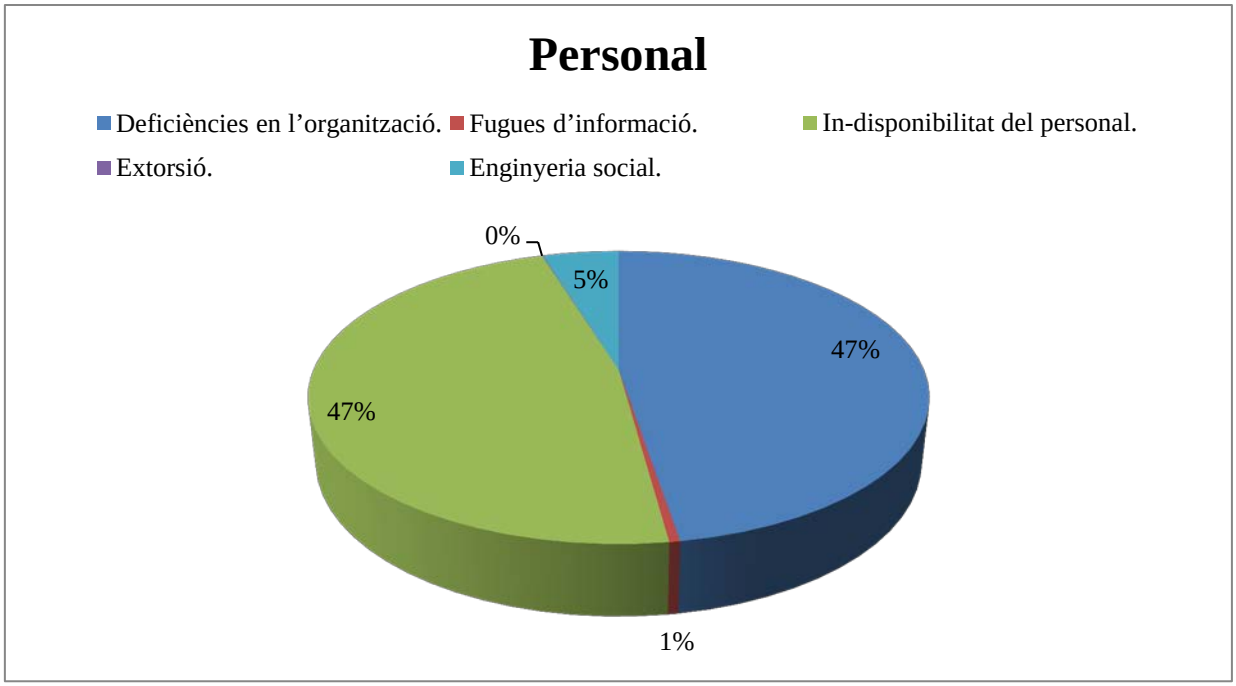
- Errors dels usuaris.
- Errors dels administradors.
- Alteració accidental de la informació.
- Destrucció de informació.
- Fuga d'informació.
- Suplantació d'identitat de l'usuari.
- Abús de privilegis d'accés.
- Ús no previst.
- Alteració de seqüència.
- Accés no autoritzat.
- Repudi.
- Modificació deliberada de la informació.
- Destrucció de informació.
- Divulgació de informació.
- Denegació de servei.



Equipament Auxiliar

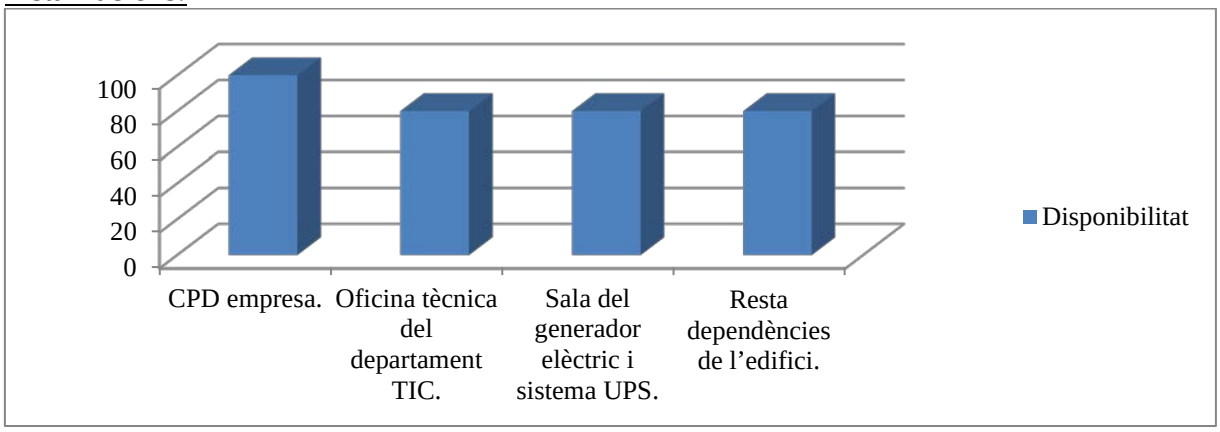
- Foc.
- Dany per aigua.
- Foc.
- Dany per aigua.
- Averia d'origen físic o lògic.
- Tall de subministrament elèctric.
- Condicions inadequades de temperatura i humitat.
- Interrupció d'altres serveis i subministres essencials.
- Errors de manteniment / actualització d'equips.
- Pèrdua d'equips.
- Ús no previst.
- Accés no autoritzat.
- Manipulació dels equips.
- Robatori.
- Atac destructiu.



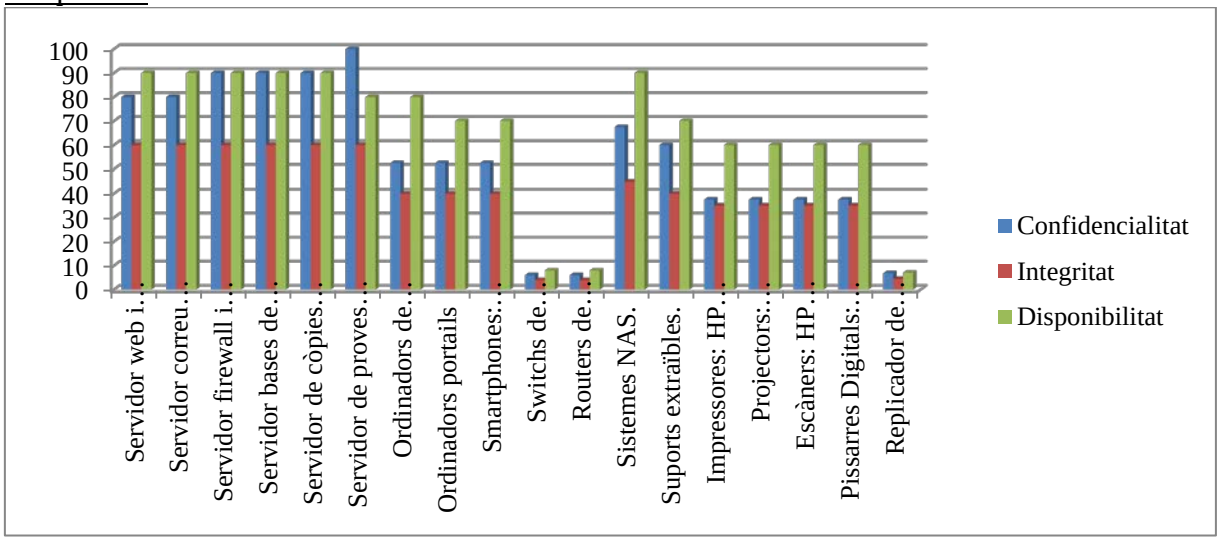


Així mateix també podem veure el risc acumulat en els diferents elements:

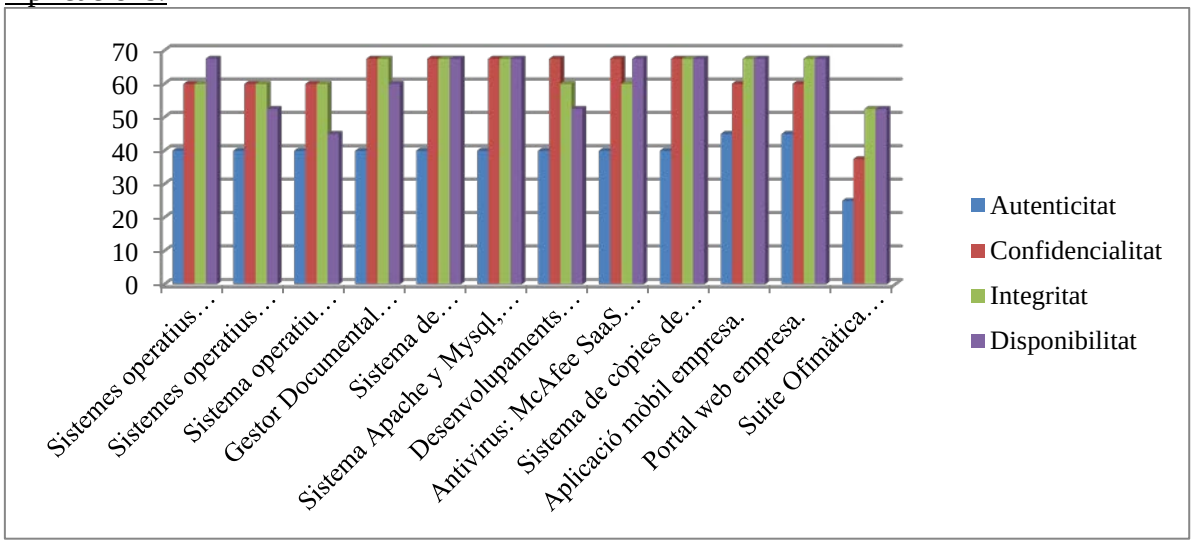
Instal·lacions:



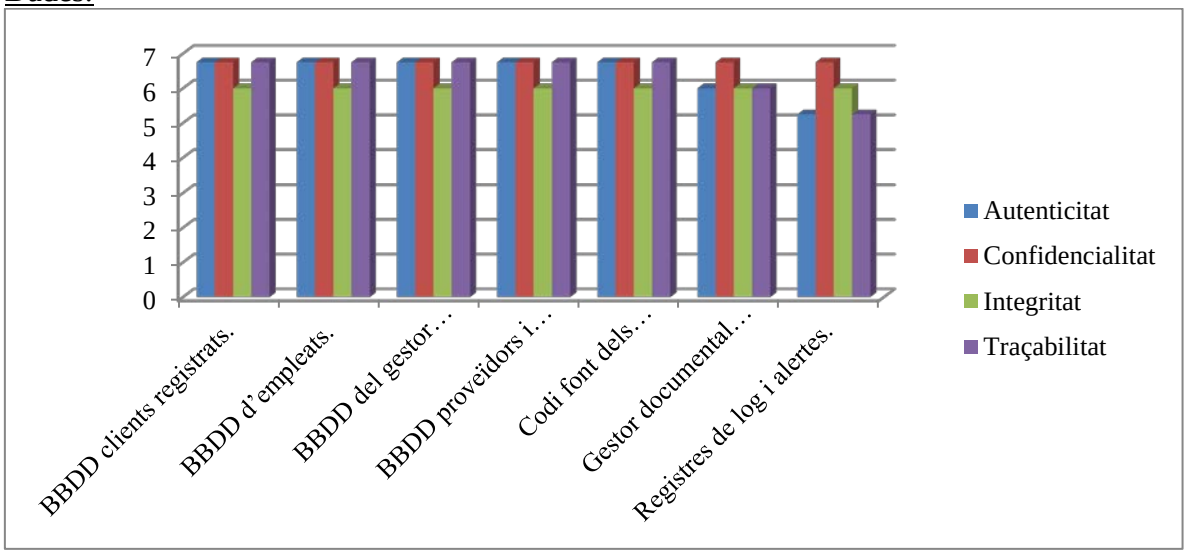
Maquinari:



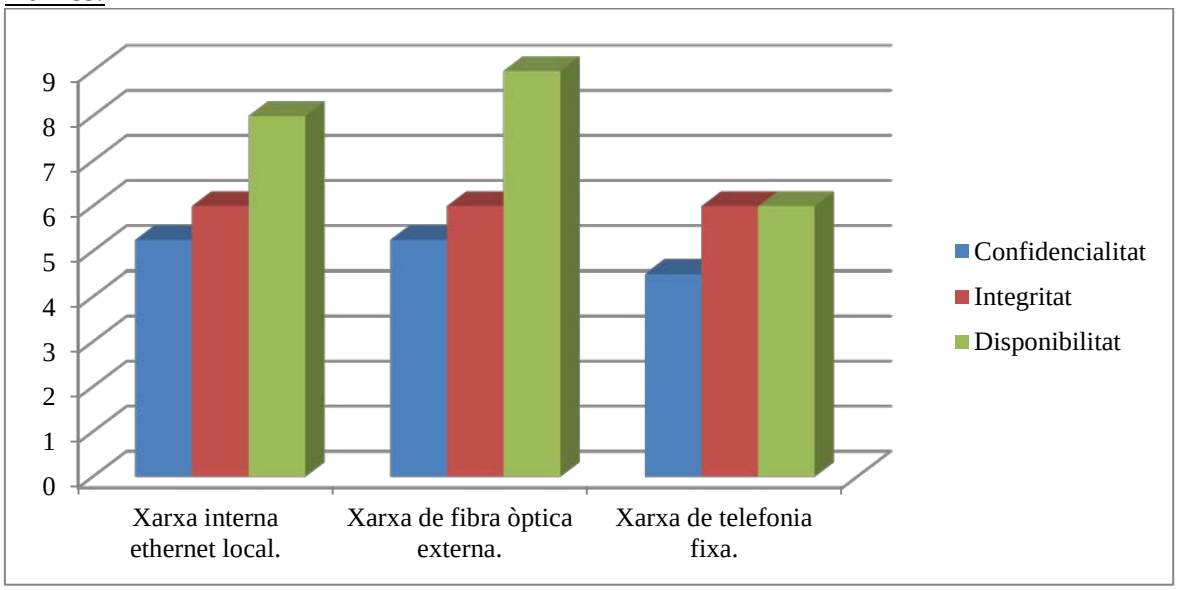
Aplicacions:



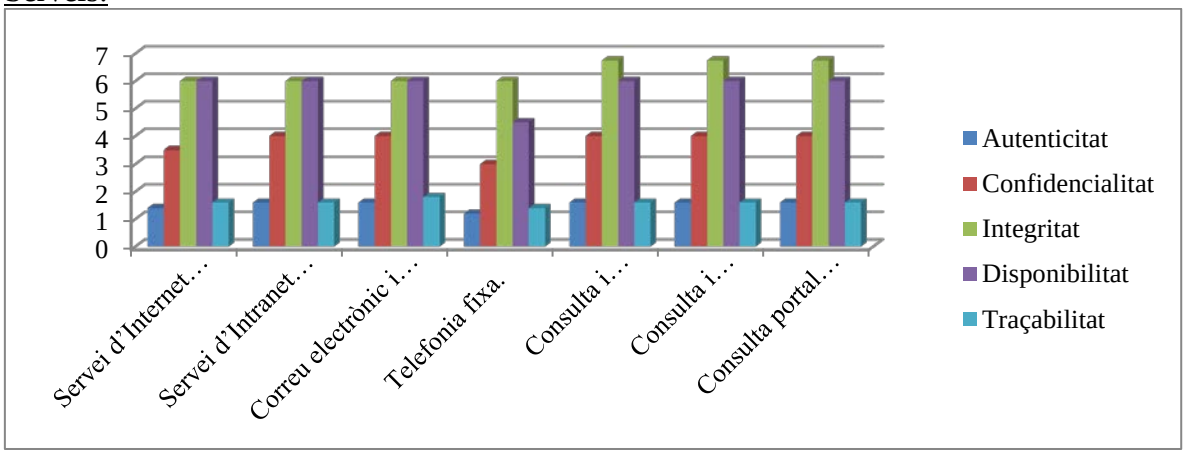
Dades:



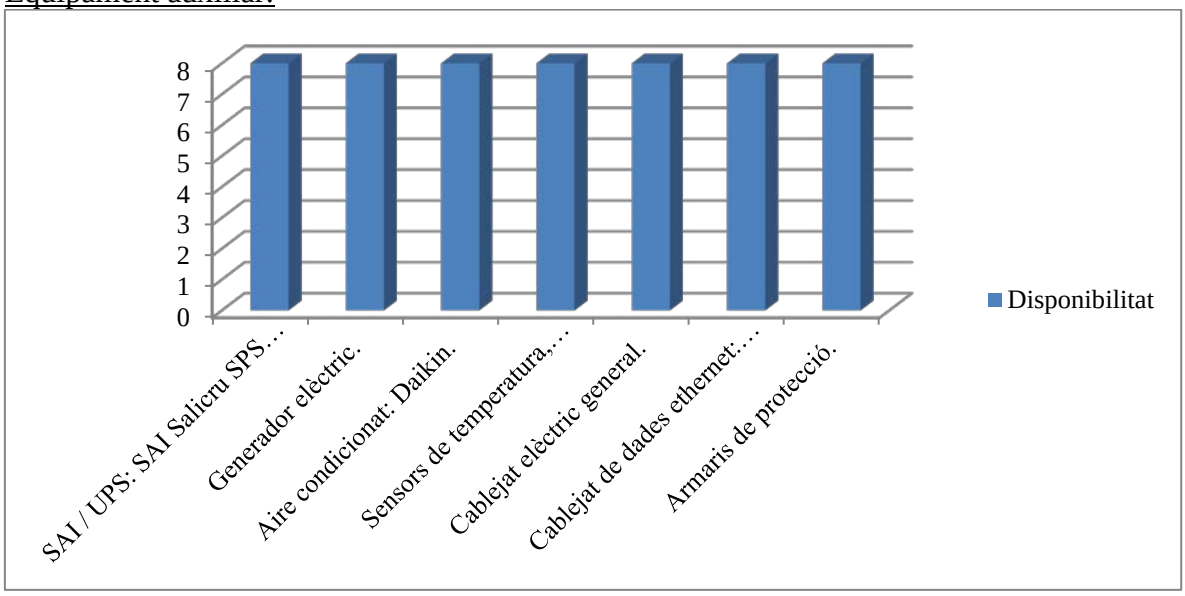
Xarxes:



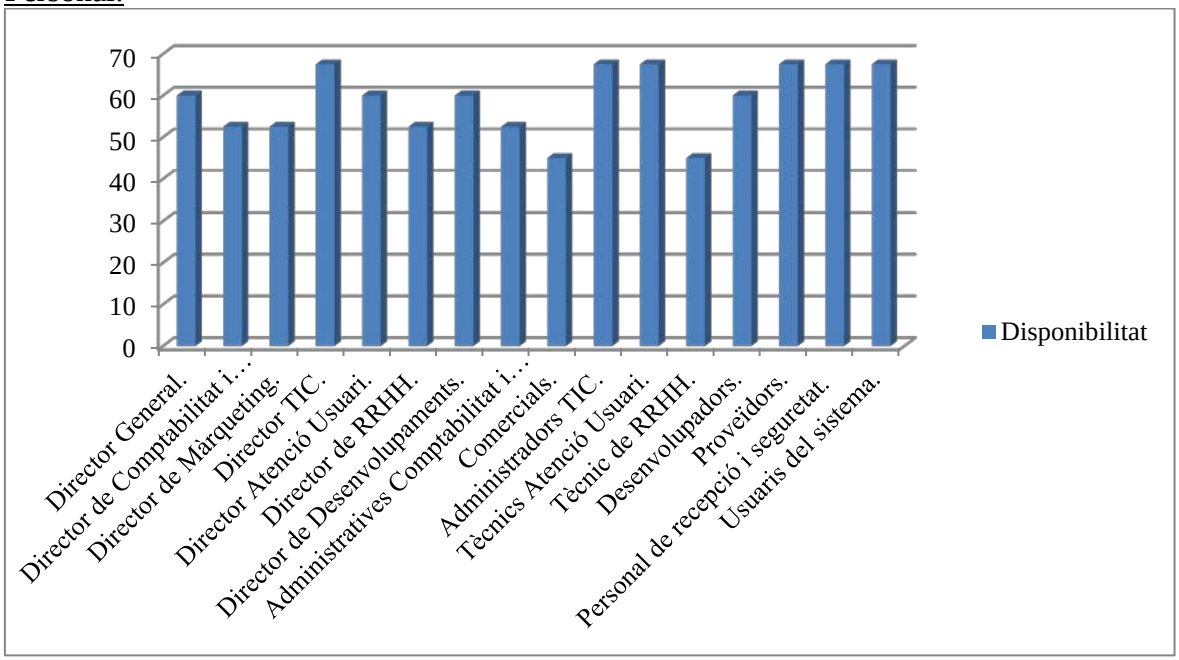
Serveis:



Equipament auxiliar:



Personal:



4. FASE IV – Propostes de projectes:

4.1. Introducció:

En la fase de propostes de projectes, ja som coneixedors dels riscs actuals que té la nostra empresa i organització i hem pogut realitzar l'anàlisi de riscs, i és el moment idoni de plantejar els projectes que permetran la millora de la seguretat dels sistemes de l'empresa.

Els diferents projectes proposats ajudaran a millorar i controlar el risc, evolucionant cap el ple compliment de la normativa ISO.

Aquests projectes, a part de millorar en els riscos identificats, també ens permetran obtenir d'altres beneficis, com pot ser la millora de la gestió de la seguretat, optimització de recursos dels sistema, millora de les tecnologies utilitzades, o millora de l'organització i dels elements relacionats amb els recursos humans.

Addicionalment, es quantificaran aquests projectes temporalment (amb un diagrama de Gantt) i econòmicament (amb un pressupost) per poder decidir si ens interessa realitzar la inversió, tenint en compte la relació millora i cost associat. A més, aquests projectes ens permetran disposar en el nostre sistema de gestió de seguretat de la informació d'un procés real de millora continua, essencial en qualsevol organització responsable i conscienciada de que la seva seguretat és molt important.

4.2. Objectius dels projectes proposats:

El fet de presentar nous projectes per a realitzar-los té com a principals objectius, minimitzar els riscos que hem identificat fins a un nivell que la nostre organització pugui considerar que és acceptable, així com contribuir a una adopció de millors pràctiques, tant per l'organització, com pels seus empleats, oferir noves eines que permetin millorar la seguretat de l'empresa, i finalment també podem considerar com a important que permetin millorar les diferents dimensions, com són la autenticitat, confidencialitat, integritat, disponibilitat i traçabilitat, de cadascun dels diferents actius de que disposa l'empresa, i que hem identificat degudament en apartats anteriors.

I tot això sense oblidar, que el que persegueix qualsevol empresa que desitgi una bona seguretat dels seus actius és que és porti a terme un procés de millora continua o cicle de Deming (PDCA).

4.3. Abast dels projectes proposats:

L'abast dels projectes busca millorar la seguretat i evitar la possible materialització de les amenaces a que esta sotmesa l'empresa, i per tant, l'abast es centrarà a resoldre les debilitats i vulnerabilitats identificades en el nostres actius que formin part del sistema d'informació de l'empresa, els elements inter-relacionats, els empleats, els processos, i qüestions organitzacionals de l'empresa.

Per tant, en molts casos dels següents projectes podrem veure que un mateix projecte pot millorar altres conceptes i aportar avantatges a d'altres elements, tant directament com indirectament, aportant una major seguretat a diferents elements del sistema.

4.4. Propostes:

En els següents apartats podrem veure els detalls dels projectes proposats:

4.4.1. Proposta de projecte 1 – Redundància del sistema elèctric, i del cablejat:

4.4.1.1. Identificació del projecte:

Codi: PROJ_RED_ELE_1.

4.4.1.2. Nom del projecte:

Nom: Redundància del sistema elèctric, i del cablejat.

4.4.1.3. Abast del projecte:

El projecte abastarà tots els actius de les instal·lacions i dels equipaments auxiliars, ja sigui maquinari dels empleats, servidors, CPD, i sistemes de control.

4.4.1.4. Objectius i avantatges del projecte:

Els principals objectius i avantatges del projecte seran els següents:

- Disposar d'un sistema elèctric redundant per tot el sistema.
- Evitar pèrdues d'informació per causa elèctrica.
- Evitar pèrdues de maquinari per causa elèctrica.
- Evitar una pèrdua de seguretat de les instal·lacions per causa elèctrica (evitant perdre sensors, càmeres, il·luminació, detecció...)
- Evitar pèrdues de disponibilitat temporal per causa elèctrica.
- Evitar pèrdues econòmiques per causa elèctrica.
- Disponibilitat del 100% del sistema en cas de fallada d'algun component elèctric, ja que el disposem redundat, i la seva activació seria immediata.
- No s'atura la seguretat del sistema durant qualsevol incidència elèctrica en un dels dos sistemes redundats.
- No perdem dades, ni maquinari per sobretensions, o caigudes del sistema.
- El personal de manteniment disposa de temps de resposta menor en cas d'incidents elèctrics, i pot solucionar la incidència en l'equip redundat, mentre l'altre dona servei correctament.

4.4.1.5. Descripció i tasques del projecte:

El projecte vol crear un sistema redundant d'energia elèctrica, que eviti possibles caigudes del sistema, amb les conseqüents pèrdues de informació, i pèrdues materials i temporals de maquinari, que puguin ser causades tant per sobretensions, baixes tensions, pics de consum, i hores vall, o fenòmens naturals i industrials que puguin afectar el sistema elèctric de l'empresa.

Durant el projecte és realitzarà un anàlisi de les instal·lacions elèctriques i de les necessitats, una cerca de proveïdors que puguin realitzar el projecte, una quantificació precisa del temps estimat i del cost exacte del projecte, l'aprovació del projecte final per part de direcció, la posada en marxa del projecte, i finalment l'avaluació dels resultats del projecte.

4.4.1.6. Cost econòmic del projecte:

El cost econòmic del projecte serà el següent:

- Instal·lació del generador i del cablejat: 2.000€.
- Cost del nou cablejat: 1.000€.
- Cost del grup electrogen industrial (per exemple, Taigüer 100Kva): 9.084 €. (http://www.taiguergeneradores.com/catalogo/grupos-electrogenos-29/grupos-electrogenos-insonorizados-31/)

Total: **12.084 €**

4.4.1.7. Durada aproximada del projecte:

La durada aproximada dependrà dels possibles problemes de instal·lació del cablejat redundat i de les instal·lacions elèctriques noves, i de l'entrega dels generadors adquirits per part dels proveïdors, però s'estima que pot estar instal·lat i en ple funcionament en un període de **3 mesos**.

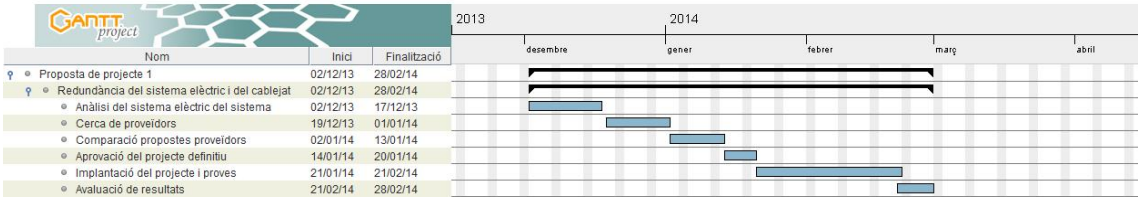
4.4.1.8. Relació amb l'anàlisi de riscs:

Amb relació amb l'anàlisi de riscs, obtenim una millora en l'apartat de disponibilitat dels actius de les instal·lacions, maquinari, servidors, CPD, i equipament auxiliar, que augmenta la disponibilitat en casos de l'amenaça de falta d'energia elèctrica.

En l'ISO 27002, obtenim una millora en l'apartat: 9.Seguretat física i de l'entorn.

4.4.1.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



Nom	Inici	Finalització
Proposta de projecte 1	02/12/13	28/02/14
Redundància del sistema elèctric i del cablejat	02/12/13	28/02/14
Anàlisi del sistema elèctric del sistema	02/12/13	17/12/13
Cerca de proveïdors	19/12/13	01/01/14
Comparació propostes proveïdors	02/01/14	13/01/14
Aprovació del projecte definitiu	14/01/14	20/01/14
Implantació del projecte i proves	21/01/14	21/02/14
Avaluació de resultats	21/02/14	28/02/14

4.4.2. Proposta de projecte 2 – Formació dels empleats i usuaris:

4.4.2.1. Identificació del projecte:

Codi: PROJ_FOR_EMP_2.

4.4.2.2. Nom del projecte:

Nom: Formació dels empleats i usuaris.

4.4.2.3. Abast del projecte:

L'abast del projecte afectarà a tots els empleats i usuaris directes que treballen per l'empresa i que fan servir el sistema d'informació, que veuran millorada la seva formació.

4.4.2.4. Objectius i avantatges del projecte:

Els objectius i avantatges que aconseguim amb aquest projecte seran els següents:

- Millora de la conscienciació de les millors practiques en el lloc de treball.
- Millora de la formació en les noves tècniques en seguretat.
- Millora en la seguretat de les dades i de les aplicacions.
- Millora en el coneixement de la documentació de seguretat de l'empresa.
- Millora en la seguretat dels equips, les dades i les aplicacions.
- Reducció de les incidències relacionades amb el personal de l'empresa.

4.4.2.5. Descripció i tasques del projecte:

La formació busca aconseguir un millor coneixement de les tècniques de seguretat, i bones pràctiques en l'entorn de treball, per evitar incidències, i millorar la seguretat general del treball, millorant la falta de formació que actualment existeix en l'empresa.

Durant la realització del projecte s'elaborarà un pla de formació, es cercaran els professionals més adequats que poden realitzar les sessions de formació, s'aprovaran, per part de direcció els diferents cursos proposats, es portaran a terme els esmentats cursos segons els perfils d'usuaris, i finalment s'avaluaran els plans de formació per part de direcció i dels diferents empleats que hi han participat, per obtenir-ne l'èxit del projecte.

4.4.2.6. Cost econòmic del projecte:

El cost econòmic del projecte serà el següent:

- Materials: 300€, en concepte de quaderns, fotocopies, i estris diversos d'escriptura.

- Dependències: 0€, ja que es cediran les sales de reunions com a sales de formació mentre duri la formació, ja que estan equipades amb projector, i pissarra digital, cadires i taules suficients.

- Professor: 30€/hora, i disposarem de 4 grups de formació: directius de departament, empleats dels departaments, departament TIC, i desenvolupadors.

    - 30€/hora * 16 sessions * 2 hores cada sessió * 4 grups = 3.840€

Per tant, el cost directe del projecte serà de 3.840 + 200€ = **4.040€**

4.4.2.7. Durada aproximada del projecte:

La durada aproximada del projecte de formació serà de 4 mesos, amb 1 sessió setmanal pels diferents perfils d'usuaris, amb un total de 16 sessions de formació. Addicionals als 2 mesos anteriors de preparació del pla de formació, i cerca i comparació de professionals. Posteriorment, hi haurà 1 mes d'avaluació. Amb un total del projecte de **7 mesos**.

Les sessions es realitzaran segons els perfils d'usuaris en horaris que minimitzin les possibles afectacions al treball diari de cada treballador.

4.4.2.8. Relació amb l'anàlisi de riscs:

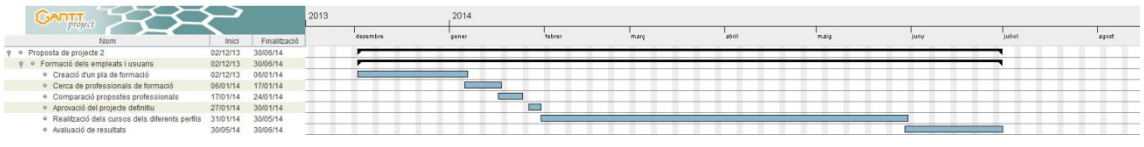
Amb relació amb l'anàlisi de riscos, la formació en seguretat dels diferents perfils, ajudarà a l'empresa a millorar les dimensions d'autenticitat, confidencialitat, la seva integritat, i a reduir errors no intencionats d'usuaris i administradors.

I pel que fa referència a la ISO 27002, obtenim millores remarcables en:

- 8.2.2. Conscienciació i capacitació en seguretat de la informació.
- 11.3.1. Ús de contrasenyes.
- 11.3.2. Equip d'usuari desatès.
- 11.3.3. Política de lloc de treball buit i pantalla neta.
- 15.1.5. Prevenció d'ús indegut dels recursos de tractament de la informació.
- 15.2.1. Compliment de les polítiques i normes de seguretat.

4.4.2.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



4.4.3. Proposta de projecte 3 – Millora de la salut en el treball i de l'organització de la seguretat:

4.4.3.1. Identificació del projecte:

Codi: PROJ_SAL_ORG_3.

4.4.3.2. Nom del projecte:

Nom: Millora de la salut en el treball i de l'organització de la seguretat.

4.4.3.3. Abast del projecte:

L'abast del projecte afectarà a l'organització i a la salut general del lloc de treball de tots els treballadors de l'empresa, i dels diferents departaments, tenint en compte les seves particularitats, que l'equip que realitzi el projecte haurà de detectar i tenir en compte.

4.4.3.4. Objectius i avantatges del projecte:

Tot seguit podem veure alguns dels avantatges i objectius que persegueix el projecte:

- Millora de la seguretat física en el lloc de treball.
- Millora de la salut dels treballadors amb l'ús de bons hàbits.
- Millora de l'organització de càrrecs dels departaments involucrats amb la seguretat del sistema, concretament, creació del càrrec de responsable de seguretat del sistema.
- Millora de la disponibilitat dels treballadors, per la reducció de baixes motivades per mals hàbits, i falta de bones pràctiques en l'estació de treball.

4.4.3.5. Descripció i tasques del projecte:

El projecte cercarà la millora contínua del lloc de treball i de l'organització de l'empresa i de possibles nous llocs de treball per suplir possibles deficiències detectades, per exemple la nova creació del lloc de responsable de seguretat del sistema.

A més cercarà millorar la seguretat física i de l'entorn, realitzant tasques per mantenir o millorar aquestes bones pràctiques, assignant els recursos eficientment i millorant els processos que necessitin revisió, per tant serà un projecte que pot esdevenir en un futur en sub-projectes que tractin temes relacionats.

Entre les tasques del projecte, s'haurà de revisar l'organització, els processos, les tasques, els recursos, la seguretat i salut de l'entorn, i contractar una empresa que realitzi les millores necessàries (com per exemple, podria ser en el cas més simple, canviar cadires incomodes per cadires ergonòmiques, per perfils d'empleats que es passen moltes hores assentats, i que poden derivar a baixes per mals d'esquena), l'empresa realitzarà les diferents tasques detectades, implantarà les millores aprovades

per direcció, i finalment, n'obtindrà un feedback dels diferents perfils implicats per poder detectar l'èxit del projecte.

4.4.3.6. Cost econòmic del projecte:

El cost econòmic del projecte serà el següent:

- Contractació d'una empresa de millora de salut laboral: 3.000€
- Xerrades per part d'un professional a tots els treballadors de les mesures: 300€
- Creació del nou lloc de treball de responsable de seguretat: 2.800€ / mensuals.
- Equip informàtic del treballador: 0€, ja que l'empresa en té disponibles.

Cost total del projecte: **3.300€ directes + 2.800€ de nòmina mensual del treballador**.

4.4.3.7. Durada aproximada del projecte:

La durada aproximada del projecte serà de **6 mesos**, tenint en compte que s'haurà de realitzar un estudi previ, i posteriorment aplicar les millores en salut i organització, que suposin millores remarcables en la feina.

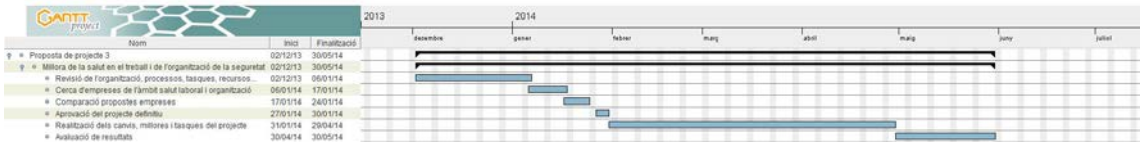
4.4.3.8. Relació amb l'anàlisi de riscs:

Amb aquest projecte obtindrem millores en l'anàlisi de riscos en la dimensió de la disponibilitat del personal de l'empresa, ja que una correcte organització i un correcte lloc de treball disminuirà les baixes laborals, i incidirà en una reducció de les incidències reportades per errors no intencionats produïts per usuaris i administradors.

En referència a la ISO 27002 obtenim millores en: 9.Seguretat física i de l'entorn.

4.4.3.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



4.4.4. Proposta de projecte 4 – Millora de l'actualització, suport i manteniment:

4.4.4.1. Identificació del projecte:

Codi: PROJ_MIL_ASM_4.

4.4.4.2. Nom del projecte:

Nom: Millora de l'actualització, suport i manteniment.

4.4.4.3. Abast del projecte:

El projecte abastarà tots els sistemes de maquinari del CPD, del servidor, dels equips personals, dispositius portàtils, i smartphones. Així com les diferents aplicacions, i sistemes operatius dels sistemes esmentats.

4.4.4.4. Objectius i avantatges del projecte:

Aquest projecte ens imposarà una sèrie d'objectius i avantatges:

- Reducció d'incidències causades per falta de manteniment.
- Millora de la solució de les incidències en un temps menor, gràcies a un millor suport.
- Reducció d'errors dels equips dins el programa de manteniment.
- Millora de la seguretat del diferent maquinari.
- Millora de la seguretat de les dades.
- Millora de la seguretat de les diferents aplicacions.
- Millora directe i indirecta de la seguretat dels empleats.
- Implantació immediata de les diferents actualitzacions als diferents programaris del sistema.

4.4.4.5. Descripció i tasques del projecte:

El present projecte mira de implantar solucions de manteniment continu, de manera que el sistema, les aplicacions i totes les dades gaudeixin d'un manteniment, implantació d'actualitzacions i suport millorat.

Les tasques del projecte seran les d'analitzar les necessitats de manteniment, nivell d'actualització actual i desitjat, i suport, per tal que l'equip de direcció pugui aprovar els nivells. El departament TIC serà l'encarregat de responsabilitzar-se del manteniment dels equips i de la instal·lació de les actualitzacions. Així mateix el departament també realitzarà el suport tècnic en el cas del report de les diferents incidències que els

diferents perfils d'usuaris indiquin del sistema. Periòdicament es realitzaran auditories internes per tal de comprovar el correcte funcionament del projecte.

Com a tasques addicionals també és realitzaran proves per poder demostrar el correcte funcionament del sistema.

4.4.4.6. Cost econòmic del projecte:

El cost econòmic del projecte serà el següent:

10.000€ anuals per processos de millora d'equips de forma ordinària + **"X"€** anuals que podran ser aprovats per direcció per millores extraordinàries (canvis de servidors, canvis en el CPD de cost superior...)

4.4.4.7. Durada aproximada del projecte:

El manteniment no disposa d'un termini concret, ja que s'haurà de realitzar de forma **continuada i periòdica** en el temps, mentre els sistemes de l'empresa estiguin en funcionament.

4.4.4.8. Relació amb l'anàlisi de riscs:

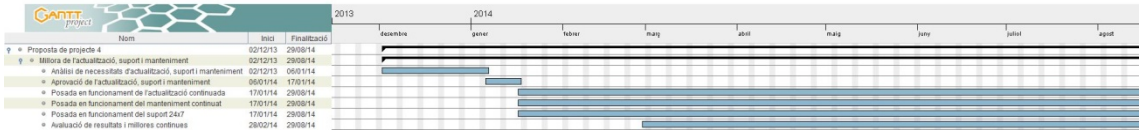
Amb relació a l'anàlisi de riscs, el manteniment, actualitzacions i suport, millorarà les dimensions de seguretat de la confidencialitat, integritat del maquinari. Així mateix també millorarà la dimensió d'autenticitat, confidencialitat i integritat de les aplicacions, i les dades que s'utilitzen en aquestes aplicacions. El suport tècnic millorarà la disponibilitat del personal, de les instal·lacions, de les aplicacions i del maquinari, ja que estarà un menor temps aturat en cas d'incidència tècnica.

Respecte a la ISO 27002 obtenim millores en:

- 6.Aspectes organitzatius de la seguretat de la informació.
- 9. Seguretat física i de l'entorn.
- 12. Adquisició, desenvolupament i manteniment dels sistemes de informació.

4.4.4.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



(no es visualitzen els finals de les línies del diagrama de Gantt, per simbolitzar el concepte de funcionament continu del projecte al llarg del temps).

4.4.5. Proposta de projecte 5 – Continuïtat del negoci i gestió d'incidències:

4.4.5.1. Identificació del projecte:

Codi: PROJ_CON_NEG_5.

4.4.5.2. Nom del projecte:

Nom: Continuïtat del negoci i gestió d'incidències.

4.4.5.3. Abast del projecte:

L'abast del projecte es centrarà en tot el sistema d'informació, posant especial èmfasi en els actius més vulnerables i en els més sensibles pel sistema, així com la seva gestió.

4.4.5.4. Objectius i avantatges del projecte:

El projecte es centrarà en els següents objectius i avantatges:

- Poder tenir un pla de contingència davant un desastre que pugui afectar el sistema.
- Poder gestionar totes les incidències, i registrar-les adequadament.
- Poder actuar ràpidament davant de qualsevol incidència detectada.
- Poder augmentar la disponibilitat del sistema.
- Poder oferir un millor servei als usuaris dels sistema.
- Minimitzar l'impacte en l'organització, i la reacció immediata del personal de seguretat i del departament TIC davant de les incidències.
- Poder realitzar plans de prova i recuperació i evolucionar-los per cadascun del sistemes i actius involucrats.
- Tenir una gestió directa del risc i control dels actius.

4.4.5.5. Descripció i tasques del projecte:

El projecte es centrarà a crear un pla de continuïtat del sistema, per poder evitar que una situació adversa tingui un efecte molt negatiu en el sistema, i puguem assegurar que els principals sistemes i aplicacions continuaran funcionant normalment en el cas d'una incidència, i per tant, afectar al mínim els usuaris. Aquest fet augmentarà la satisfacció i confiança del sistema per part del usuaris del portal web i de l'aplicació mòbil, i dels mateixos treballadors de l'empresa, i tindrem una gestió més ràpida de les incidències.

Les tasques principals del projecte, serà l'anàlisi de tots els sistemes, per poder detectar quines són les tasques del sistema que són més essencials i que necessiten ser més protegits per el pla de continuïtat del sistema, posteriorment, el crearà l'esmentat pla i

els projectes que se'n derivin s'enviaran a direcció per poder ser aprovats i millorar la seguretat del sistema, i en últim pas, el sistema ja disposarà del pla, per revisar-lo periòdicament en les següents auditories que es realitzin (amb les corresponents proves de funcionament), ja que el sistema segueix un sistema de millora contínua.

4.4.5.6. Cost econòmic del projecte:

El cost econòmic del projecte és podrà subdividir en els següents elements:

- 2 empleats que realitzin, i documentin el projecte de continuïtat del negoci (200h estimades amb un cost de 15€/h = 3.000€).

- 1 responsable que supervisi el projecte (50h estimades amb un cost de 25€/h = 1.250€).

Amb un total de cost del personal: 3.000€ + 1.250€ = **4.250€**

Un cop el projecte ja s'ha realitzat, el departament de direcció l'haurà de dotar dels recursos econòmics suficients per poder realitzar les accions que se'n derivin.

4.4.5.7. Durada aproximada del projecte:

El procés de creació i anàlisi del projecte s'estima que tindrà una durada aproximada de 5 mesos, amb una estimació de 3 mesos més per realitzar-ne les implantacions i millores necessàries. Amb un total de **8 mesos**.

D'altra banda la continuïtat del negoci és un procés que s'ha d'anar revisant i incorporant al negoci de manera permanent amb totes les millores necessàries, ja que només d'aquesta forma el funcionament serà òptim.

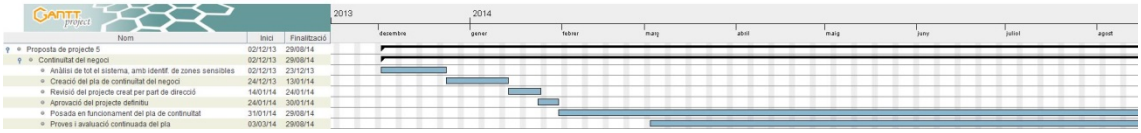
4.4.5.8. Relació amb l'anàlisi de riscs:

Amb relació amb l'anàlisi de riscos, la continuïtat del negoci permetrà millorar molt les dimensions de disponibilitat de tots els actius del sistema, de manera que per una incidència aconseguim que no es vegi afectat tot el sistema, ni actius relacionats o dependents amb el que ha fallat.

Així mateix, respecte a la ISO 27002, té relació amb: 14. Gestió de la continuïtat del negoci, i addicionalment amb 13. Gestió d'incidents de la seguretat.

4.4.5.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



(no es visualitzen els finals de les línies del diagrama de Gantt, per simbolitzar el concepte de funcionament continu del projecte al llarg del temps).

4.4.6. Proposta de projecte 6 – Millora de la documentació, divulgació i compliment (disciplinari):

4.4.6.1. Identificació del projecte:

Codi: PROJ_MILL_DDC_6.

4.4.6.2. Nom del projecte:

Nom: Millora de la documentació, divulgació i compliment.

4.4.6.3. Abast del projecte:

El projecte abastarà tota la documentació del sistema, aplicacions, processos, i sistema d'organització, normatives i polítiques de seguretat, i la seva divulgació entre tot el personal involucrat en els diferents perfils d'usuaris de l'empresa.

4.4.6.4. Objectius i avantatges del projecte:

Els principals objectius dels projecte seran els següents:

- Fomentar la creació de documentació de tots els sistemes, aplicacions, processos, i organització de l'empresa, amb les normatives i polítiques relacionades.

- Fomentar la seva divulgació entre tot el personal de l'empresa, de manera que tots els treballadors en tinguin accés.

- Fomentar que les normatives i polítiques de seguretat siguin conegudes pels diferents perfils de treballadors.

- Assegurar que tots els treballadors compleixen les normatives i polítiques de seguretat.

- Dissenyar i activar un protocol d'actuació disciplinaria, de manera que la direcció pugui actuar en el cas d'incompliment d'alguna de les normatives o polítiques de seguretat.

- Dissenyar un protocol d'actuació en cas de detecció d'alguna actitud o manera de fer que pugui ser constitutiva de delicte (forma de contacte amb autoritats policials i unitats judicials), tant pel personal de l'empresa, com pels usuaris de l'aplicació web i del portal web.

- Assegurar les proves detectades mitjançant la implantació de tècniques d'informàtica forense.

4.4.6.5. Descripció i tasques del projecte:

El projecte consistirà a la creació de les diferents documentacions, polítiques i normatives, divulgació intensiva de les mateixes, i creació i activació del procés disciplinari. Així mateix també s'establiran paràmetres de gestió d'actius, com són la millora de l'inventari, propietaris, o responsables dels actius.

Com a tasques del projecte, podem detallar que existiran les d'anàlisi del sistema, processos, aplicacions, per posteriorment revisar-ne i crear-ne (si encara no existeix) la documentació, així mateix existirà després la divulgació de la citada documentació, polítiques i normatives, i per finalitzar amb l'activació de tot el procés disciplinari.

4.4.6.6. Cost econòmic del projecte:

El cost econòmic del projecte serà el següent:

- Creació de nova documentació i revisió de la documentació actual creada del sistema, processos i aplicacions. 2 empleats (50h a 10€/h x 2): 1.000€.

- Creació de polítiques i normatives de seguretat. 2 empleats (50h a 10€/h x 2): 1.000€.

- Creació del protocol d'actuació disciplinari i contacte amb autoritats. 2 empleats (30h a 10€/h x 2): 600€.

Cost total del projecte: 1.000€ + 1.000€ + 600€ = **2.600€**

4.4.6.7. Durada aproximada del projecte:

La durada aproximada del projecte serà de 4 mesos, per la creació de la documentació, les polítiques, normatives, i el protocol d'actuació disciplinari. Addicionalment s'habilitaran 3 mesos de divulgació intensiva de les normatives i de les polítiques, abans de la seva posada en funcionament definitiva. Per tant, la durada total del projecte serà de **7 mesos**.

4.4.6.8. Relació amb l'anàlisi de riscs:

Amb relació amb l'anàlisi de riscs, podem dir que una major divulgació i una nova i millor documentació del sistema permetrà que apareguin un menor nombre d'errors no intencionats produïts en els sistemes i per usuaris i administradors, per tant millorarà la dimensió de la disponibilitat, i integritat del sistemes.

Addicionalment, una més clara organització dels sistemes i processos permetrà que la dimensió de disponibilitat del personal també augmenti en el cas de l'amenaça de deficiències en l'organització que es va contemplar en el citat anàlisi de riscos.

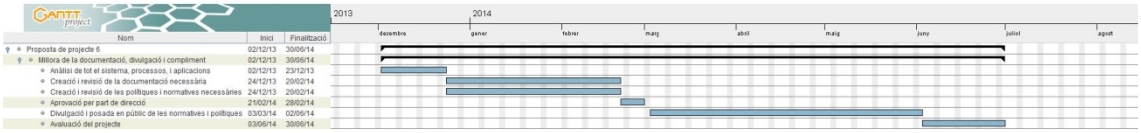
Amb relació a la ISO 27002, té relació amb:

- 5. Política de seguretat.
- 7. Gestió d'actius.
- 8.2.2. Conscienciació, formació i capacitació en seguretat de la informació.

- 8.2.3. Procés disciplinari.
- 10.1.1. Documentació dels procediments d'operació.
- 15. Compliment.

4.4.6.9. Diagrama de Gantt del projecte:

Tot seguit podem veure el diagrama de Gantt estimat pel projecte:



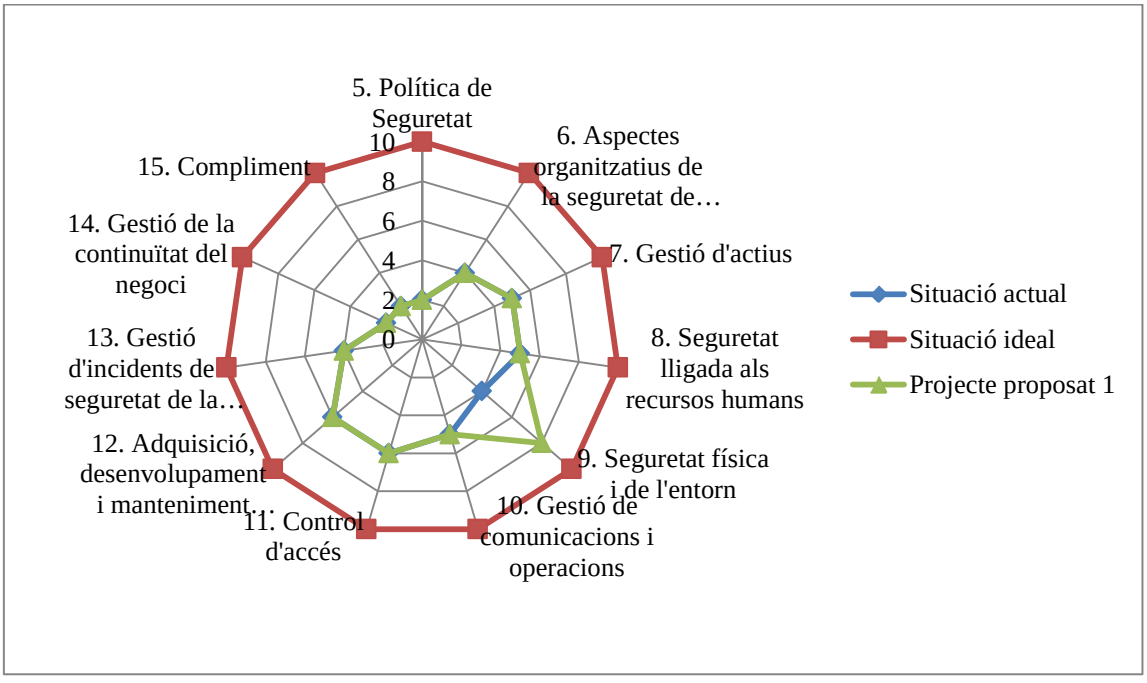
4.5. Resultats:

Un cop hem realitzat una proposta dels diferents projectes que ens pot interessar implantar en l'empresa o organització, mostrarem mitjançant un diagrama de radar l'evolució, amb el compliment abans i després de la realització dels projectes proposats. Així com també el nivell ideal de compliment de cada variable.

Per la realització dels gràfics utilitzarem les següents dades de la **situació actual estimada**, la situació ideal, i la **millora estimada** aportada pels diferents projectes. Així mateix en els requadres de dades tindrem en compte que s'ha quantificat l'estat del 0 al 10, que equival del 0% al 100% d'estat de compliment ideal.

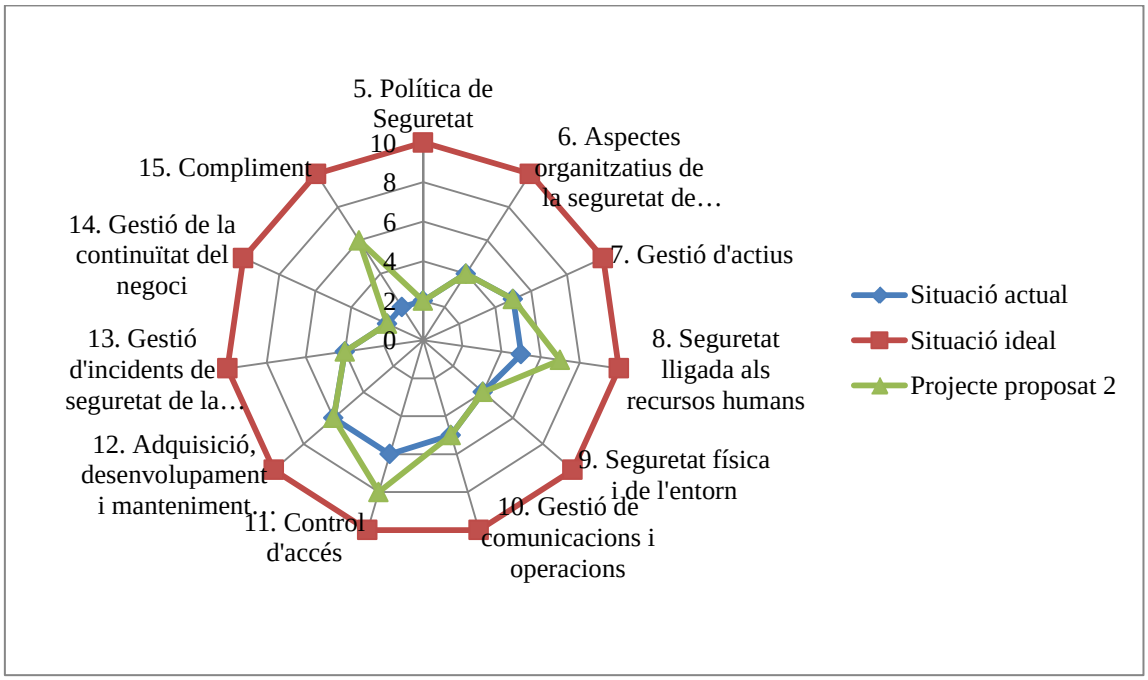
En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 1: Redundància del sistema elèctric, i del cablejat.

ISO 27002	Situació actual	Situació ideal	Projecte proposat 1
5. Política de Seguretat	2	10	2
6. Aspectes organitzatius de la seguretat de la informació	4	10	4
7. Gestió d'actius	5	10	5
8. Seguretat lligada als recursos humans	5	10	5
9. Seguretat física i de l'entorn	4	10	8
10. Gestió de comunicacions i operacions	5	10	5
11. Control d'accés	6	10	6
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	6
13. Gestió d'incidents de seguretat de la informació	4	10	4
14. Gestió de la continuïtat del negoci	2	10	2
15. Compliment	2	10	2



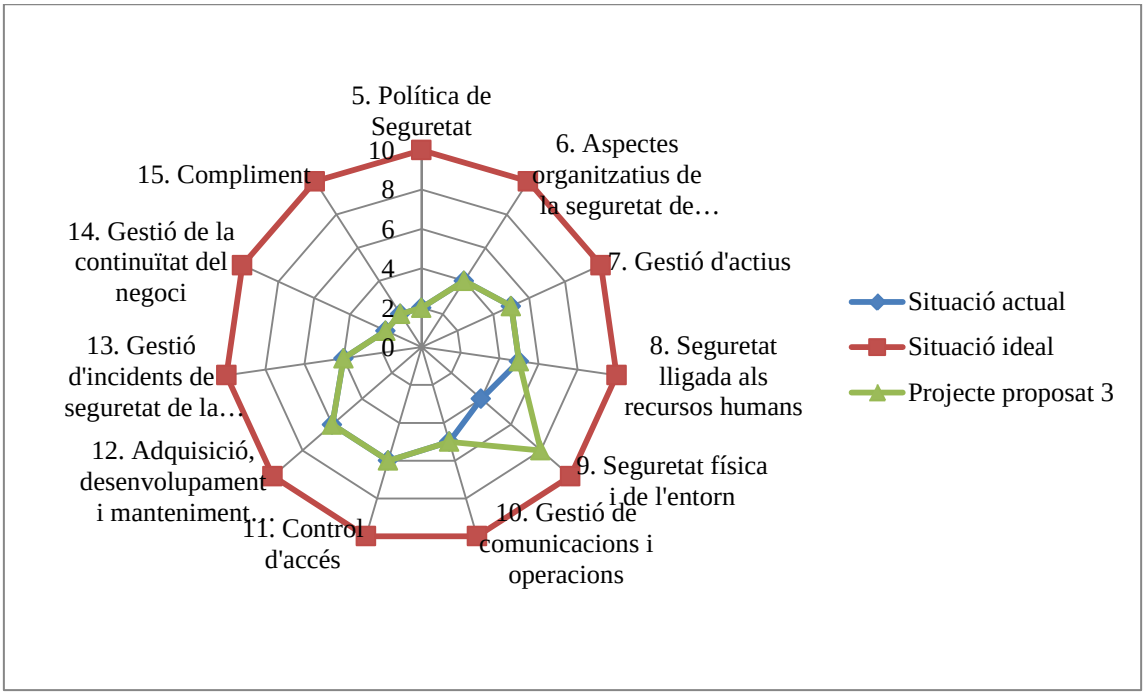
En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 2: Formació dels empleats i usuaris.

ISO 27002	Situació actual	Situació ideal	Projecte proposat 2
5. Política de Seguretat	2	10	2
6. Aspectes organitzatius de la seguretat de la informació	4	10	4
7. Gestió d'actius	5	10	5
8. Seguretat lligada als recursos humans	5	10	7
9. Seguretat física i de l'entorn	4	10	4
10. Gestió de comunicacions i operacions	5	10	5
11. Control d'accés	6	10	8
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	6
13. Gestió d'incidents de seguretat de la informació	4	10	4
14. Gestió de la continuïtat del negoci	2	10	2
15. Compliment	2	10	6



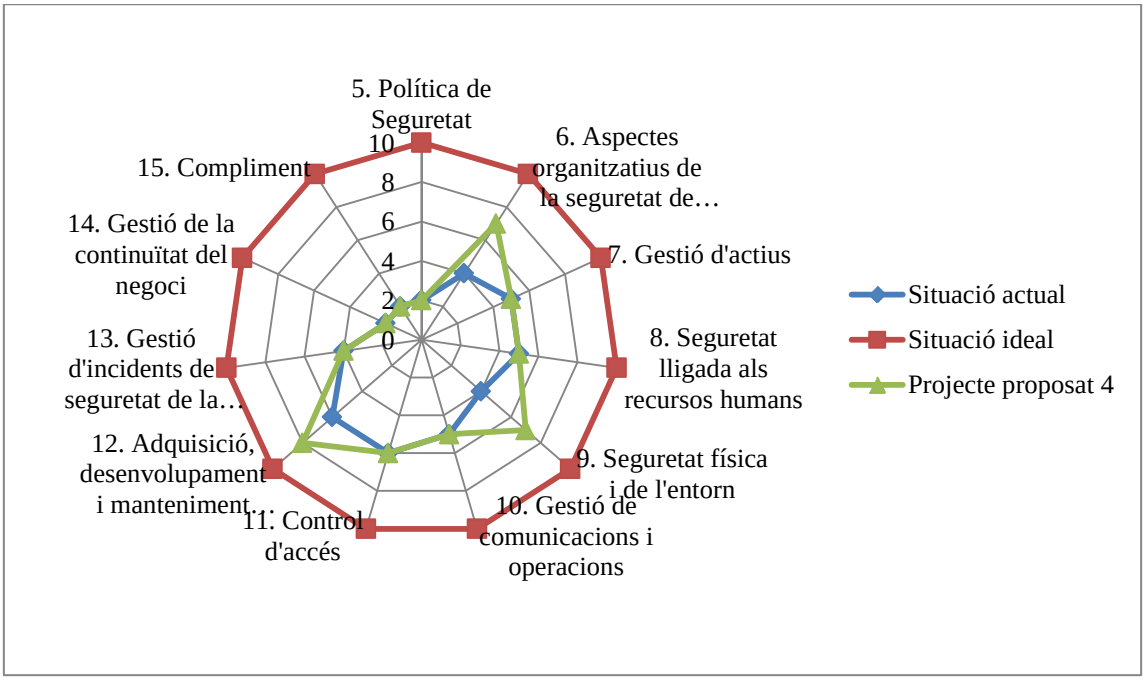
En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 3: Millora de la salut en el treball i de l'organització de la seguretat.

ISO 27002	Situació actual	Situació ideal	Projecte proposat 3
5. Política de Seguretat	2	10	2
6. Aspectes organitzatius de la seguretat de la informació	4	10	4
7. Gestió d'actius	5	10	5
8. Seguretat lligada als recursos humans	5	10	5
9. Seguretat física i de l'entorn	4	10	8
10. Gestió de comunicacions i operacions	5	10	5
11. Control d'accés	6	10	6
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	6
13. Gestió d'incidents de seguretat de la informació	4	10	4
14. Gestió de la continuïtat del negoci	2	10	2
15. Compliment	2	10	2



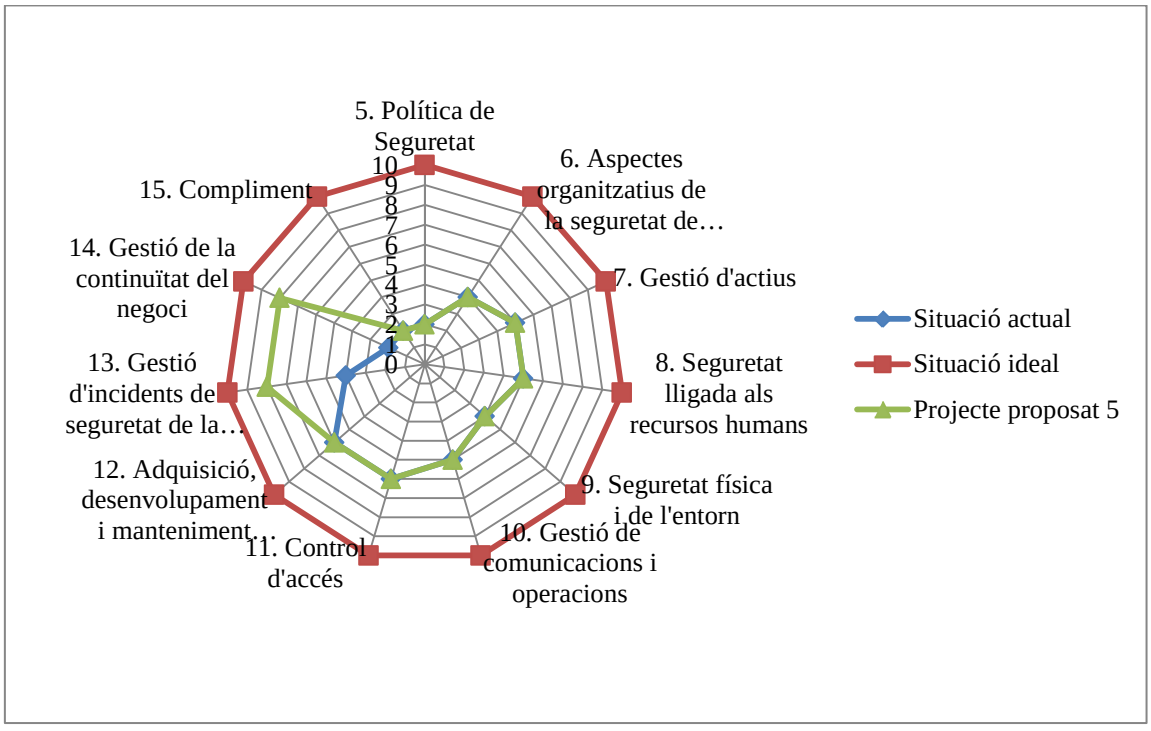
En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 4: Millora de l'actualització, suport i manteniment.

ISO 27002	Situació actual	Situació ideal	Projecte proposat 4
5. Política de Seguretat	2	10	2
6. Aspectes organitzatius de la seguretat de la informació	4	10	7
7. Gestió d'actius	5	10	5
8. Seguretat lligada als recursos humans	5	10	5
9. Seguretat física i de l'entorn	4	10	7
10. Gestió de comunicacions i operacions	5	10	5
11. Control d'accés	6	10	6
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	8
13. Gestió d'incidents de seguretat de la informació	4	10	4
14. Gestió de la continuïtat del negoci	2	10	2
15. Compliment	2	10	2



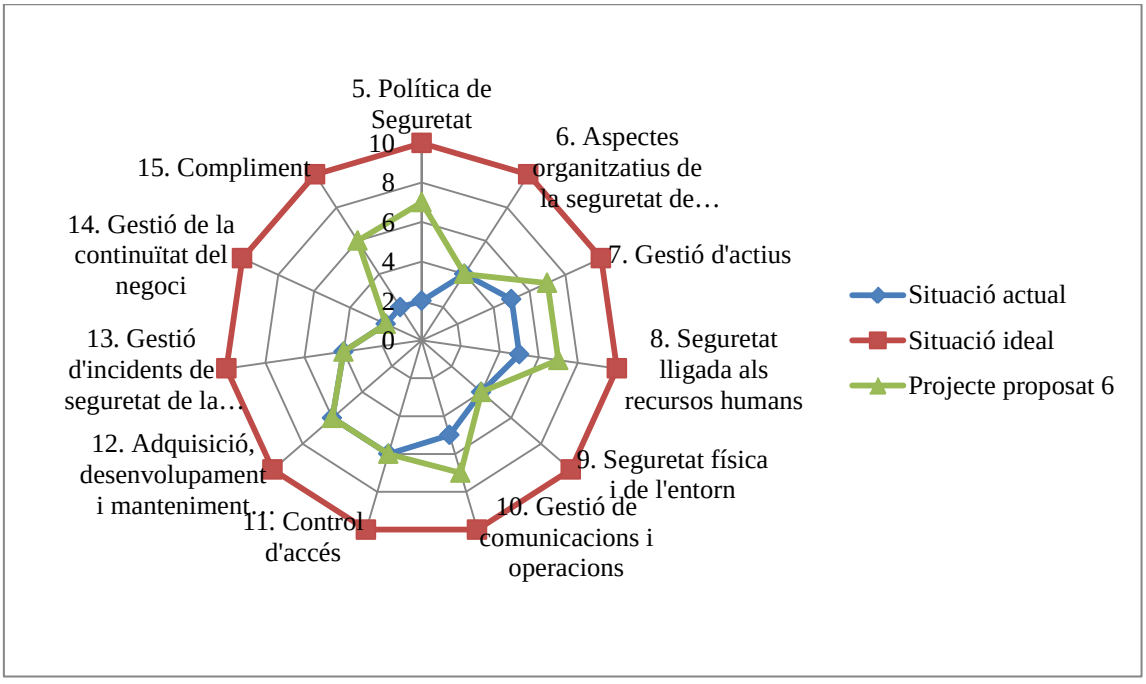
En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 5: Continuïtat del negoci i gestió d'incidències.

ISO 27002	Situació actual	Situació ideal	Projecte proposat 5
5. Política de Seguretat	2	10	2
6. Aspectes organitzatius de la seguretat de la informació	4	10	4
7. Gestió d'actius	5	10	5
8. Seguretat lligada als recursos humans	5	10	5
9. Seguretat física i de l'entorn	4	10	4
10. Gestió de comunicacions i operacions	5	10	5
11. Control d'accés	6	10	6
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	6
13. Gestió d'incidents de seguretat de la informació	4	10	8
14. Gestió de la continuïtat del negoci	2	10	8
15. Compliment	2	10	2



En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportaria el projecte proposat 6: Millora de la documentació, divulgació i compliment.

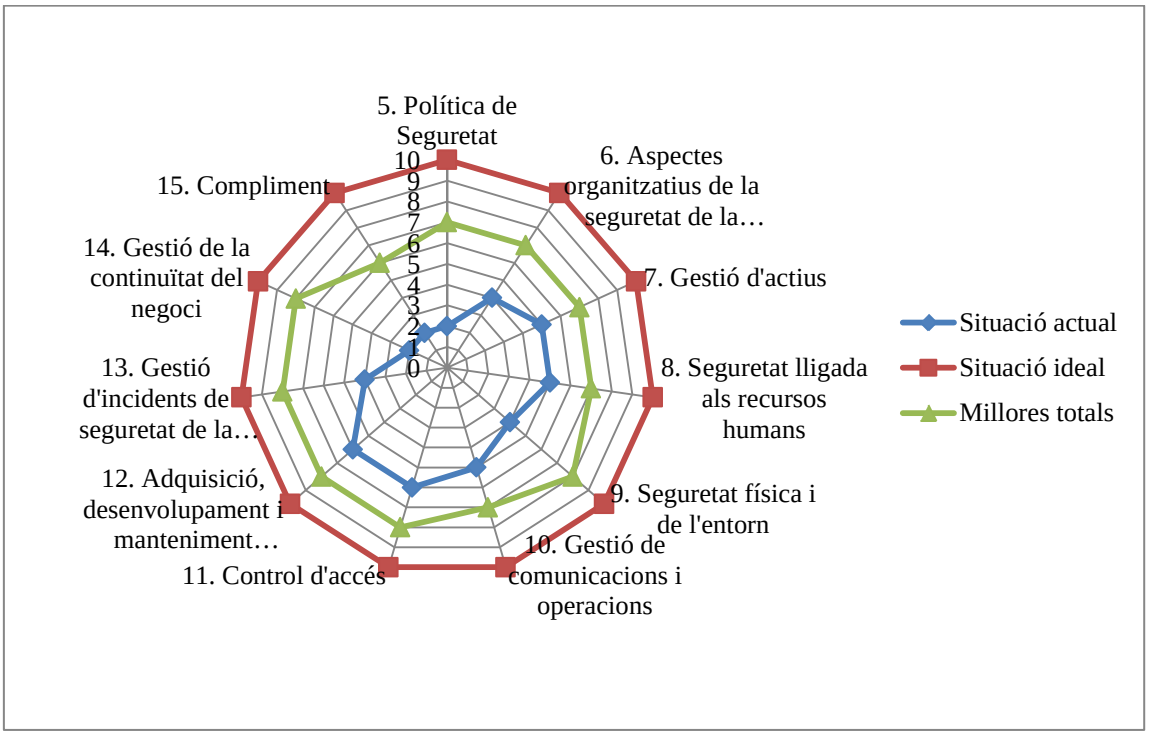
ISO 27002	Situació actual	Situació ideal	Projecte proposat 6
5. Política de Seguretat	2	10	7
6. Aspectes organitzatius de la seguretat de la informació	4	10	4
7. Gestió d'actius	5	10	7
8. Seguretat lligada als recursos humans	5	10	7
9. Seguretat física i de l'entorn	4	10	4
10. Gestió de comunicacions i operacions	5	10	7
11. Control d'accés	6	10	6
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	6
13. Gestió d'incidents de seguretat de la informació	4	10	4
14. Gestió de la continuïtat del negoci	2	10	2
15. Compliment	2	10	6



En el següent gràfic podem observar el diagrama de radar amb les millores estimades que ens aportarien si es consideres oportú realitzar tots els projectes proposats.
Com podem observar, amb els diferents projectes proposats aconseguiríem una notable millora de les diferents variables, i augmentaríem considerablement la seguretat del sistema, **acostant-nos al valor de la situació ideal de cara a una pròxima fase d'auditoria interna i una posterior auditoria externa pel compliment de la ISO.**

Evidentment, durant el transcurs dels diferents projectes, poden sorgir-ne d'altres relacionats o no relacionats, que podrien fer augmentar els valors, i que en cada cas s'hauria d'estudiar i demanar-ne l'aprovació de direcció, per si estima convenient dotar-los de nous recursos, depenent del valor de millora i el cost relacionat amb cadascun.

ISO 27002	Situació actual	Situació ideal	Millores totals (valor màxim dels projectes 1 al 6 (max(X1...X6))
5. Política de Seguretat	2	10	7
6. Aspectes organitzatius de la seguretat de la informació	4	10	7
7. Gestió d'actius	5	10	7
8. Seguretat lligada als recursos humans	5	10	7
9. Seguretat física i de l'entorn	4	10	8
10. Gestió de comunicacions i operacions	5	10	7
11. Control d'accés	6	10	8
12. Adquisició, desenvolupament i manteniment dels sistemes d'informació	6	10	8
13. Gestió d'incidents de seguretat de la informació	4	10	8
14. Gestió de la continuïtat del negoci	2	10	8
15. Compliment	2	10	6



5. FASE V – Auditoria de Compliment de la ISO/IEC 27002:

5.1. Introducció:

En aquesta última fase, ara que ja tenim identificades de forma clara les amenaces, els elements i actius vulnerables de l'organització, i ho hem pogut constatar mitjançant l'anàlisi de riscos, així com també hem pogut proposar alguns dels més importants o destacables projectes que poden millorar la seguretat del sistema d'informació, és el moment idoni d'avaluar l'empresa per saber si compleix amb les bones pràctiques de seguretat que ens proposa la ISO/IEC 27002, i que ens servirà per saber l'estat actual dels controls de seguretat de l'empresa.

5.2. Data i lloc de realització:

La auditoria es realitzarà durant el transcurs de la última fase d'aquest projecte, en el marc temporal de desembre de 2013 i gener de 2014. El lloc de realització serà a les pròpies oficines que els responsables de l'empresa cediran per poder portar a terme satisfactòriament l'auditoria, així com a les pròpies oficines de l'empresa certificadora.

5.3. Abast de la certificació:

L'abast de la certificació es centrarà en tot el sistema d'informació de l'empresa, la seva infraestructura, els seus actius, els equipaments auxiliars, el maquinari, el programari, les dades, els serveis, les xarxes, i el personal. Així com també amb els diferents elements interrelacionats amb la seguretat i organització dels processos i elements que interactuen en el procés productiu o de serveis de l'empresa.

5.4. Tipus d'auditoria

X	Inicial
	Seguiment
	Renovació
	Ampliació
	Extraordinària (indicar el motiu)

5.5. Normativa aplicable:

En aquesta auditoria es tindrà en compte la normativa ISO 27001:2005, així com el catàleg de controls de la ISO 27002.

5.6. Metodologia:

La ISO/IEC 27002, que és un estàndard internacional, disposa d'un total de 133 controls que ens permeten tenir bones pràctiques de la gestió de la seguretat de la informació. Aquests controls estan organitzats en 11 àrees i 39 objectius de control.

Les mesures preventives que redueixen el risc poden actuar en diferents aspectes:

- Creació de la documentació, i normes que l'empresa i que els seus responsables haurà de revisar i aprovar.

- Polítiques del personal de l'empresa.
- Sol·licituds tècniques de programari, maquinari i comunicacions.
- Seguretat física de l'empresa i dels actius.

Els dominis de control de la ISO/IEC 27002 que s'analitzaran seran:

- [5.] Política de seguretat.
- [6.] Organització de la seguretat de la informació.
- [7.] Gestió actius.
- [8.] Seguretat dels recursos humans.
- [9.] Seguretat física i ambiental.
- [10.] Gestió de comunicacions i operacions.
- [11.] Control d'accés.
- [12.] Adquisició, desenvolupament i manteniment dels sistemes de informació.
- [13.] Gestió d'incidents.
- [14.] Gestió de la continuïtat del negoci.
- [15.] Compliment.

La següent taula ens permet veure la metodologia que s'utilitzarà per descriure el compliment dels diferents controls de la ISO/IEC 27002:

Efectivitat	CMM	Significat	Descripció
0%	**L0**	Inexistent	Carència completa de qualsevol procés que reconeguem. No s'ha reconegut que existeixi cap problema a resoldre.
10%	**L1**	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. Els procediments son inexistents o localitzats en àrees concretes. No existeixen plantilles definides a nivell

			corporatiu
50%	**L2**	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca. Es normalitzen les "bones practiques" en base a l'experiència i al mètode. No hi ha comunicació o entreteniment formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	**L3**	Procés definit	La organització sencera participa al procés. Els processos estan implantats, documentats i comunicats mitjançant entreteniment.
95%	**L4**	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, s'ha de tenir eines per a millorar la qualitat i la eficiència.
100%	**L5**	Optimitzat	Els processos estan sota constant millora. En base criteris quantitatius es determinen les desviacions més comunes i s'optimitzen els processos.

5.7. Taula de compliment dels controls ISO/IEC 27002:

Tot seguit podem veure la taula de compliment de la ISO/IEC 27002, amb els valors de efectivitat, i el valor CMM que s'estima per cadascun dels diferents tipus de controls.

ISO 27002 – TAULA DE COMPLIMENT		
Tipus de Control ISO	**Efectivitat**	**CMM**
[5.] Política de seguretat	**90%**	**L3**
[5.1.] Política de seguretat de la informació	**90%**	**L3**
[5.1.1.] Document de política de seguretat de la informació	**90%**	**L3**
[5.1.2.] Revisió de la política de seguretat de la informació	**90%**	**L3**
[6.] Aspectes organitzatius de la seguretat de la informació	**84,41%**	**>L2<L3**
[6.1.] Organització interna	**92,14%**	**>L3<L4**
[6.1.1.] Compromís de la direcció amb la seguretat de la informació	**100%**	**L5**
[6.1.2.] Coordinació de la seguretat de la informació	**95%**	**L4**
[6.1.3.] Assignació de responsabilitats relatives a la seguretat	**90%**	**L3**

de la informació		
[6.1.4.] Procés d'actualització de recursos pel tractament de la informació	**90%**	**L3**
[6.1.5.] Acords de confidencialitat	**90%**	**L3**
[6.1.6.] Contacte amb les autoritats	**90%**	**L3**
[6.1.7.] Contacte amb grups d'especial interès	**NO APLICA**	
[6.1.8.] Revisió independent de la seguretat de la informació	**90%**	**L3**
[6.2.] Tercers	**76,67%**	**>L2<L3**
[6.2.1.] Identificació dels riscos derivats de l'accés de tercers	**50%**	**L2**
[6.2.2.] Tractament de la seguretat en la relació amb els clients	**90%**	**L3**
[6.2.3.] Tractament de la seguretat en contractes amb tercers	**90%**	**L3**
[7.] Gestió d'actius	**92,5%**	**>L3<L4**
[7.1.] Responsabilitat sobre els actius	**95%**	**L4**
[7.1.1.] Inventari d'actius	**95%**	**L4**
[7.1.2.] Propietat dels actius	**95%**	**L4**
[7.1.3.] Ús acceptable dels actius	**95%**	**L4**
[7.2.] Classificació de la informació	**90%**	**L3**
[7.2.1.] Directrius de classificació	**90%**	**L3**
[7.2.2.] Etiquetat i manipulat de la informació	**90%**	**L3**
[8.] Seguretat lligada als recursos humans	**95%**	**L4**
[8.1.] Abans de la feina	**100%**	**L5**
[8.1.1.] Funcions i responsabilitats	**100%**	**L5**
[8.1.2.] Investigació d'antecedents	**100%**	**L5**
[8.1.3.] Termes i condicions de contractació	**100%**	**L5**
[8.2.] Durant la feina	**95%**	**L4**
[8.2.1.] Responsabilitats de la direcció	**100%**	**L5**
[8.2.2.] Conscienciació, formació i capacitació en seguretat de la informació	**95%**	**L4**
[8.2.3.] Procés disciplinari	**90%**	**L3**
[8.3.] Finalització de la feina o canvi de lloc de treball	**90%**	**L3**
[8.3.1.] Responsabilitat de finalització o canvi	**90%**	**L3**
[8.3.2.] Devolució d'actius	**90%**	**L3**
[8.3.3.] Retirada de drets d'accés	**90%**	**L3**
[9.] Seguretat física i de l'entorn	**87,14%**	**>L2<L3**
[9.1.] Àrees segures	**90%**	**L3**
[9.1.1.] Perímetre de seguretat física	**90%**	**L3**
[9.1.2.] Controls físics d'entrada	**90%**	**L3**
[9.1.3.] Seguretat d'oficines, despatxos i instal·lacions	**90%**	**L3**
[9.1.4.] Protecció contra les amenaces externes i d'origen	**90%**	**L3**

ambiental		
[9.1.5.] Treball en àrees segures	**90%**	**L3**
[9.1.6.] Àrees d'accés públic i de càrrega i descarrega	**NO APLICA**	
[9.2.] Seguretat dels equips	**84,28%**	**>L2<L3**
[9.2.1.] Distribució i protecció dels equips	**90%**	**L3**
[9.2.2.] Instal·lacions de subministrament	**90%**	**L3**
[9.2.3.] Seguretat del cablejat	**90%**	**L3**
[9.2.4.] Manteniment dels equips	**90%**	**L3**
[9.2.5.] Seguretat dels equips de fora les instal·lacions	**50%**	**L2**
[9.2.6.] Reutilització o retirada segura d'equips	**90%**	**L3**
[9.2.7.] Retirada de materials propietat de l'empresa	**90%**	**L3**
[10.] Gestió de comunicacions i operacions	**83,22%**	**>L2<L3**
[10.1.]Responsabilitats i procediments d'operació	**93,5%**	**>L3<L4**
[10.1.1.] Documentació dels procediments d'operació	**90%**	**L3**
[10.1.2.] Gestió de canvis	**95%**	**L4**
[10.1.3.] Segregació de tasques	**95%**	**L4**
[10.1.4.] Separació dels recursos de desenvolupament, prova i operació	**95%**	**L4**
[10.2.] Gestió de la provisió de serveis per tercers	**NO APLICA**	
[10.2.1.] Provisió de serveis	**NO APLICA**	
[10.2.2.] Supervisió i revisió dels serveis oferts per tercers	**NO APLICA**	
[10.2.3.] Gestió del canvi en els serveis oferts per tercers	**NO APLICA**	
[10.3.] Planificació i acceptació del sistema	**95%**	**L4**
[10.3.1.] Gestió de capacitats	**95%**	**L4**
[10.3.2.] Acceptació del sistema	**95%**	**L4**
[10.4.] Protecció contra el codi maligne i descarregues	**90%**	**L3**
[10.4.1.] Controls contra el codi maligne	**90%**	**L3**
[10.4.2.] Controls contra el codi descarregat en el client	**90%**	**L3**
[10.5.] Copies de seguretat	**50%**	**L2**
[10.5.1.] Copies de seguretat de la informació	**50%**	**L2**
[10.6.] Gestió de la seguretat de les xarxes	**90%**	**L3**
[10.6.1.] Controls de xarxa	**90%**	**L3**
[10.6.2.] Seguretat dels serveis de xarxa	**90%**	**L3**
[10.7.] Manipulació dels suports	**70%**	**>L2<L3**
[10.7.1.] Gestió de suports extraïbles	**50%**	**L2**
[10.7.2.] Retirada de suports	**50%**	**L2**
[10.7.3.] Procediments de manipulació de la informació	**90%**	**L3**
[10.7.4.] Seguretat de la documentació del sistema	**90%**	**L3**

[10.8.] Intercanvi de informació	**68%**	**>L2<L3**
[10.8.1.] Polítiques i procediments de intercanvi de informació	**50%**	**L2**
[10.8.2.] Acords de intercanvi	**50%**	**L2**
[10.8.3.] Suports físics en transit	**50%**	**L2**
[10.8.4.] Missatgeria electrònica	**95%**	**L4**
[10.8.5.] Sistemes de informació empresarial	**95%**	**L4**
[10.9.] Serveis de comerç electrònic	**95%**	**L4**
[10.9.1.] Comerç electrònic	**95%**	**L4**
[10.9.2.] Transaccions en línia	**95%**	**L4**
[10.9.3.] Informació públicament disponible	**95%**	**L4**
[10.10.] Supervisió	**97,5%**	**>L4<L5**
[10.10.1.] Registres d'auditoria	**90%**	**L3**
[10.10.2.] Supervisió de l'ús del sistema	**95%**	**L4**
[10.10.3.] Protecció de la informació dels registres	**100%**	**L5**
[10.10.4.] Registres d'administració i operació	**100%**	**L5**
[10.10.5.] Registre de fallades	**100%**	**L5**
[10.10.6.] Sincronització de rellotge	**100%**	**L5**
[11.] Control d'accés	**78,59%**	**>L2<L3**
[11.1.] Requisits de negoci pel control d'accés	**90%**	**L3**
[11.1.1.] Política de control d'accés	**90%**	**L3**
[11.2.] Gestió d'accés d'usuari	**92,5%**	**>L3<L4**
[11.2.1.] Registre d'usuari	**90%**	**L3**
[11.2.2.] Gestió de privilegis	**95%**	**L4**
[11.2.3.] Gestió de contrasenyes d'usuari	**95%**	**L4**
[11.2.4.] Revisió dels drets d'accés d'usuari	**90%**	**L3**
[11.3.] Responsabilitats d'usuari	**63,33%**	**>L2<L3**
[11.3.1.] Ús de contrasenyes	**90%**	**L3**
[11.3.2.] Equip d'usuari desatès	**50%**	**L2**
[11.3.3.] Política de lloc de treball buit i pantalla neta	**50%**	**L2**
[11.4.] Control d'accés a xarxa	**94,28%**	**>L3<L4**
[11.4.1.] Política d'ús dels serveis de xarxa	**90%**	**L3**
[11.4.2.] Autentificació d'usuari per connexions externes	**95%**	**L4**
[11.4.3.] Identificació dels equips en les xarxes	**95%**	**L4**
[11.4.4.] Diagnòstic remot i protecció dels ports de configuració	**95%**	**L4**
[11.4.5.] Segregació de les xarxes	**95%**	**L4**
[11.4.6.] Control de la connexió a la xarxa	**95%**	**L4**
[11.4.7.] Control d'encaminament (Routing) de xarxa	**95%**	**L4**
[11.5.] Control d'accés al sistema operatiu	**87,5%**	**>L2<L3**
[11.5.1.] Procediments segurs d'inici de sessió	**95%**	**L4**

[11.5.2.] Identificació i autentificació d'usuari	**95%**	**L4**
[11.5.3.] Sistema de gestió de contrasenyes	**95%**	**L4**
[11.5.4.] Ús dels recursos del sistema	**95%**	**L4**
[11.5.5.] Desconnexió automàtica de sessió	**95%**	**L4**
[11.5.6.] Limitació de temps de connexió	**50%**	**L2**
[11.6.] Control d'accés a les aplicacions i a la informació	**72,5%**	**>L2<L3**
[11.6.1.] Restricció de l'accés a la informació	**50%**	**L2**
[11.6.2.] Aïllament de sistemes sensibles	**95%**	**L4**
[11.7.] Ordinadors portàtils i teletreball	**50%**	**L2**
[11.7.1.] Ordinadors portàtils i comunicacions mòbils	**50%**	**L2**
[11.7.2.] Teletreball	**50%**	**L2**
[12.] Adquisició, desenvolupament i manteniment dels sistemes de informació	**83,33%**	**>L2<L3**
[12.1.] Requisits de seguretat dels sistemes de informació	**95%**	**L4**
[12.1.1.] Anàlisi i especificació dels requisits de seguretat	**95%**	**L4**
[12.2.] Tractament correcte de les aplicacions	**100%**	**L5**
[12.2.1.] Validació de les dades d'entrada	**100%**	**L5**
[12.2.2.] Control de processament intern	**100%**	**L5**
[12.2.3.] Integritat dels missatges	**100%**	**L5**
[12.2.4.] Validació de les dades de sortida	**100%**	**L5**
[12.3.] Controls criptogràfics	**50%**	**L2**
[12.3.1.] Política d'ús dels controls criptogràfics	**50%**	**L2**
[12.3.2.] Gestió de claus	**50%**	**L2**
[12.4.] Seguretat dels arxius del sistema	**90%**	**L3**
[12.4.1.] Control del programari en explotació	**90%**	**L3**
[12.4.2.] Protecció de les dades de prova del sistema	**90%**	**L3**
[12.4.3.] Control d'accés al codi font dels programes	**90%**	**L3**
[12.5.] Seguretat en el procés de desenvolupament i suport	**75%**	**>L2<L3**
[12.5.1.] Procediments de control de canvis	**100%**	**L5**
[12.5.2.] Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu	**100%**	**L5**
[12.5.3. Restriccions als canvis en els paquets de programari	**50%**	**L2**
[12.5.4.] Fugues de informació	**50%**	**L2**
[12.5.5.] Externalització del desenvolupament de programari	**NO APLICA**	
[12.6.] Gestió de la vulnerabilitat tècnica	**90%**	**L3**
[12.6.1.] Control de les vulnerabilitats tècniques	**90%**	**L3**
[13.] Gestió de incidents de seguretat de la informació	**95%**	**L4**
[13.1.] Notificació d'esdeveniments i punts dèbils de	**95%**	**L4**

seguretat de la informació		
[13.1.1.] Notificació d'esdeveniments de seguretat de la informació	**95%**	**L4**
[13.1.2.] Notificació de punts dèbils de seguretat	**95%**	**L4**
[13.2.] Gestió de incidents de seguretat de la informació i millores	**95%**	**L4**
[13.2.1.] Responsabilitats i procediments	**95%**	**L4**
[13.2.2.] Aprenentatge dels incidents de seguretat de la informació	**95%**	**L4**
[13.2.3.] Recopilació d'evidències	**95%**	**L4**
[14.] Gestió de la continuïtat del negoci	**94%**	**>L3<L4**
[14.1.] Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci	**94%**	**>L3<L4**
[14.1.1.] Inclusió de la seguretat de la informació en el procés de gestió de la continuïtat del negoci	**95%**	**L4**
[14.1.2.] Continuïtat del negoci i avaluació de riscs	**95%**	**L4**
[14.1.3.] Desenvolupament i implantació de plans de continuïtat que incloguin la seguretat de la informació	**95%**	**L4**
[14.1.4.] Marc de referència per la planificació de la continuïtat del negoci	**95%**	**L4**
[14.1.5.] Proves, manteniment i re-avaluació dels plans de continuïtat del negoci	**90%**	**L3**
[15.] Compliment	**93,05%**	**>L3<L4**
[15.1.] Compliment dels requisits legals	**89,17%**	**>L2<L3**
[15.1.1.] Identificació de la legislació aplicable	**100%**	**L5**
[15.1.2.] Drets de propietat intel·lectual (IPR)	**100%**	**L5**
[15.1.3.] Protecció dels documents de l'organització	**95%**	**L4**
[15.1.4.] Protecció de dades i privacitat de la informació de caràcter personal	**100%**	**L5**
[15.1.5.] Prevenció d'ús indegut dels recursos de tractament de la informació	**90%**	**L3**
[15.1.6.] Regulació dels controls criptogràfics	**50%**	**L2**
[15.2.] Compliment de les polítiques i normes de seguretat i compliment tècnic	**95%**	**L4**
[15.2.1.] Compliment de les polítiques i normes de seguretat	**95%**	**L4**
[15.2.2.] Comprovació del compliment tècnic	**95%**	**L4**
[15.3.] Consideracions sobre la auditoria dels sistemes de informació	**95%**	**L4**
[15.3.1.] Controls d'auditoria dels sistemes de informació	**95%**	**L4**
[15.3.2.] Protecció de les eines d'auditoria dels sistemes de informació	**95%**	**L4**

5.8. Resultats:

Un cop ja hem creat la taula podem veure'n els resultats dels diferents controls i el nivell de compliment del nostre sistema d'informació en relació a cadascun dels controls que inclou la ISO/IEC 27002. Tot seguit podem veure alguns gràfics i taules de resum que ens ajudaran a veure-ho de forma gràfica i poder interpretar els resultats.

5.8.1. No-conformitats majors, menors i observacions detectades:

Tot seguit podem veure les principals no-conformitats majors, menors i les observacions de les principals categories agrupades:

5.8.1.1. No-conformitats i observacions de la [5.] Política de seguretat:

Nº No-Conformitat	NC/01	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Falta d'indicadors de compliment en la política de seguretat, així com millora contínua.		**CMM**	L3
Paràgraf de la norma	[5.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
La política de seguretat està recent creada i implantada, però requereix un sistema de control futur i un sistema de millora contínua, així com també es necessiten crear indicadors numèrics i estadístics que permetin conèixer que es compleix la política de seguretat en tots els àmbits de l'empresa.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/01	**Data**	01/12/2013
Descripció de l'observació			
Sense observacions destacables.		**CMM**	L3
Paràgraf de la norma	[5.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.2. No-conformitats i observacions de la [6.] Organització de la seguretat de la informació:

Nº No-Conformitat	NC/02	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Aspectes organitzatius de la seguretat de la informació.		**CMM**	L2 i L3
Paràgraf de la norma	[6.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
S'haurien de realitzar tasques de millora de l'assignació de responsabilitats en matèria de seguretat, una millora dels acords de confidencialitat, en que tots els elements involucrats els incloguin per defecte, així com optimitzar l'efectivitat amb el contacte amb les autoritats i la creació d'una planificació de les auditories futures, així com una millora de la identificació i tractament dels riscos que poden comportar terceres parts.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/02	**Data**	01/12/2013
Descripció de l'observació			
Es podria portar a un següent nivell de la coordinació de la seguretat, de manera que les diferents persones involucrades estiguin coordinats davant qualsevol incidència amb una millora contínua.		**CMM**	L4
Paràgraf de la norma	[6.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.3. No-conformitats i observacions de la [7.] Gestió d'actius:

Nº No-Conformitat	NC/03	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Gestió d'actius, classificació de la informació.		**CMM**	L3
Paràgraf de la norma	[7.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
Es necessari un sistema que permeti mesurar que l'etiquetat i el manipulat de la informació es realitza de forma correcta per a tota la organització, ja que actualment està implantat però no es pot saber mitjançant estadística el seu correcte funcionament.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/03	**Data**	01/12/2013
Descripció de l'observació			
En la gestió d'actius i en la responsabilitat sobre els actius, es necessària un evolució cap a un sistema de millora contínua, en l'inventari d'actius, propietat i ús acceptable.		**CMM**	L4
Paràgraf de la norma	[7.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.4. No-conformitats i observacions de la [8.] Seguretat dels recursos humans:

Nº No-Conformitat	NC/04	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Seguretat lligada als recursos humans en el procés disciplinari, i en la finalització de la feina o canvi en el lloc de treball.		**CMM**	L3
Paràgraf de la norma	[8.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
S'haurà de comprovar que en el cas necessari que el procés disciplinari es porta a terme, ja que actualment només és una proposta de projecte. Així mateix, s'ha de millorar l'eficiència, i rapidesa en el procés de retorn d'actius, responsabilitat de finalització o canvi i retirada de drets d'accés.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/04	**Data**	01/12/2013
Descripció de l'observació			
Degut a que la conscienciació, formació i capacitació en seguretat de la informació s'acaba de realitzar en els cursets corresponents, s'ha de preveure en un futur que la formació sigui continuada, i amb cursets periòdics en els diferents àmbits de la seguretat.		**CMM**	L4
Paràgraf de la norma	[8.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.5. No-conformitats i observacions de la [9.] Seguretat física i ambiental:

Nº No-Conformitat	NC/05	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Seguretat física i de l'entorn.		**CMM**	L2 i L3
Paràgraf de la norma	[9.]		
Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**	
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó	
Firma	**Firma**	**Firma**	
			
Acció correctora proposada			
Primerament s'haurà de definir completament el procés de la seguretat que es necessària pels equips de fora de les instal·lacions, per evitar fugues i problemes futurs de seguretat. Així mateix també és important una millora contínua en noves tecnologies de les àrees segures de l'empresa, perímetres, controls físics, seguretat d'oficines i la seguretat dels propis equips, distribució, reutilització i el seu manteniment.		**Responsable implantació**	Cap de seguretat
		Data prevista d'implantació	01/02/2014
		Representant de l'empresa	Jordi Miró Amigó
		Firma	

Nº Observació	OB/05	**Data**	01/12/2013
Descripció de l'observació			
Sense observacions destacables.		**CMM**	**X**
Paràgraf de la norma	[9.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.6. No-conformitats i observacions de la [10.] Gestió de comunicacions i operacions:

Nº No-Conformitat	NC/06	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Millora de la protecció, les còpies de seguretat, la seguretat de les xarxes, la documentació, la manipulació dels suports, i l'intercanvi d'informació.		**CMM**	L2 i L3
Paràgraf de la norma	[10.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
En aquest cas, seria important tenir present de millorar i revisar tota la documentació d'operacions i la seguretat dels controls de xarxa i dels serveis de xarxa, així com crear un sistema de còpies de seguretat dels documents de les estacions de treball dels empleats, i dels suports que són extraïbles. Així mateix és important destruir eficientment, a baix nivell, els equips i suports que es retirin de producció. En la mateixa línia encoratgem l'organització a millorar els acords d'intercanvi, així com el control del suports físics en transit.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/06	**Data**	01/12/2013
Descripció de l'observació			
Com a observacions, es podria evolucionar cap a un nou nivell, de millora contínua en la segregació de tasques, i la separació de recursos de desenvolupament, prova i operació. Així com també, cercar, la perfecció en el programari que controla la missatgeria electrònica, els sistemes de informació empresarial, i el referent al comerç electrònic, cercant noves mesures de seguretat i certificacions de les plataformes d'intercanvi que estiguin al mercat i puguin ajudar a millorar la seguretat general davant qualsevol atac.		**CMM**	L4
Paràgraf de la norma	[10.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.7. No-conformitats i observacions de la [11.] Control d'accés:

Nº No-Conformitat	NC/07	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Les responsabilitats dels usuaris, el registre d'usuaris i la política d'ús de la xarxa, la limitació del temps de treball, la restricció d'accés a la informació i la seguretat dels ordinadors portàtils i el teletreball.		**CMM**	L2 i L3
Paràgraf de la norma	[11.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
Es important millorar el registre d'usuari per evitar tècniques de creació de comptes falsos. Així mateix, els usuaris han de tenir un procés definit i indicadors que permetin controlar l'ús de les contrasenyes dels sistemes, que ajudin a que els equips desatesos no puguin ser manipulats, i que en el lloc de treball estigui net a la vista d'altres. Es bàsic que existeixi un límit del temps de connexió del sistema, així com també que els portàtils i teletreball estiguin amb les mateixes mesures de seguretat dels equips de les oficines, ja que d'aquesta forma no s'importaran amenaces.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/07	**Data**	01/12/2013
Descripció de l'observació			
És important implantar un sistema de millora en la gestió de privilegis, i la gestió de contrasenyes d'usuari, perquè aquestes incorporin les mesures de seguretat, i les tecnologies més punteres que apareguin en el mercat, així com també en les mesures que l'empresa utilitza en el control d'accés a la xarxa i als sistemes operatius instal·lats en els equips. Es considera que l'aïllament del sistema és bo en el moment actual, però s'haurà de considerar possibles millores de en el futur que permetin un millor aïllament.		**CMM**	L4
Paràgraf de la norma	[11.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.8. No-conformitats i observacions de la [12.] Adquisició, desenvolupament i manteniment dels sistemes de informació:

Nº No-Conformitat	NC/08	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Controls criptogràfics, seguretat dels arxius del sistema, seguretat en el desenvolupament i vulnerabilitat tècnica.		**CMM**	L2 i L3
Paràgraf de la norma	[12.]		
Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**	
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó	
Firma	**Firma**	**Firma**	
			
Acció correctora proposada			
Es important definir tots els processos que poden utilitzar controls criptogràfics per millorar la seguretat, així mateix també es molt important controlar les fugues d'informació i les restriccions en els canvis en el desenvolupament i suport. També és important aplicar millores en la seguretat dels arxius del sistema, i això ho aconseguirem amb un millor control del programari en explotació, un accés totalment protegit al codi font del programari, a les dades de les proves del sistema i a les vulnerabilitats tècniques, perquè siguin del tot confidencials i només accessibles a perfils d'usuaris concrets i degudament autoritzats.		**Responsable implantació**	Cap de seguretat
		Data prevista d'implantació	01/02/2014
		Representant de l'empresa	Jordi Miró Amigó
		Firma	

Nº Observació	OB/08	**Data**	01/12/2013
Descripció de l'observació			
S'observa que és necessari aplicar un procés d'anàlisi, especificació i revisió contínua dels diferents requisits de seguretat, per tal que la seguretat del sistema sigui totalment optimitzada.		**CMM**	L4
Paràgraf de la norma	[12.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.9. No-conformitats i observacions de la [13.] Gestió d'incidents:

Nº No-Conformitat	NC/09	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Sense No-conformitats destacables.		**CMM**	**X**
Paràgraf de la norma	[13.]		
Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**	
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó	
Firma	**Firma**	**Firma**	
			
Acció correctora proposada			
Sense No-conformitats destacables.		**Responsable implantació**	Cap de seguretat
		Data prevista d'implantació	01/02/2014
		Representant de l'empresa	Jordi Miró Amigó
		Firma	

Nº Observació	OB/09	**Data**	01/12/2013
Descripció de l'observació			
Degut a les millores implantades i en el bon funcionament en la gestió de incidents en la seguretat de la informació, només es considera observar que és important que el procés de gestió d'incidents segueixi en un futur una millora contínua amb revisions dels processos de gestió de incidents amb les millors tècniques que minimitzin el temps d'aturada del sistema.		**CMM**	L4
Paràgraf de la norma	[13.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.10. No-conformitats i observacions de la [14.] Gestió de la continuïtat del negoci:

Nº No-Conformitat	NC/10	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Proves, manteniment, i re-avaluació dels plans de continuïtat del negoci.		**CMM**	L3
Paràgraf de la norma	[14.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
Es necessari crear un conjunt de proves i re-avaluar-les periòdicament perquè els plans de negoci tinguin el màxim de millores que es puguin aplicar. Aquest conjunt de proves s'han de anar avaluant en el sistema per assegurar-ne el correcte funcionament en totes les situacions possibles i en tots els escenaris que es puguin donar en un present o futur.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/10	**Data**	01/12/2013
Descripció de l'observació			
Com en tot procés acabat de crear, el model de continuïtat de negoci, necessita un període de maduració, i millora continua que el portarà a ser perfectament adaptat i provat pel sistema. Per tant, s'observa que es necessita una maduració del pla de continuïtat.		**CMM**	L4
Paràgraf de la norma	[14.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.1.11. No-conformitats i observacions de la [15.] Compliment:

Nº No-Conformitat	NC/11	**Data**	01/12/2013
NC-Major		**NC-Menor**	**X**
Descripció de la No-Conformitat			
Prevenció d'ús indegut i regulació de controls criptogràfics.		**CMM**	L2 i L3
Paràgraf de la norma	[15.]		

Representant de l'empresa	**Nom de l'auditor**	**Nom de l'auditor en cap**
Jordi Miró Amigó	Jordi Miró Amigó	Jordi Miró Amigó
Firma	**Firma**	**Firma**
		

Acció correctora proposada		
Cal una millora efectiva de la regulació dels controls criptogràfics, amb la utilització de noves tècniques pioneres d'encriptació, que ajudin als diferents àmbits a tenir els sistemes amb el màxim grau de seguretat necessari per cada casuística que podem trobar en l'empresa auditada. Així mateix l'ús indegut dels recursos ha de millorar a un procés que permeti seguir-ne l'evolució amb metodologies estadístiques i amb indicadors per controlar-ne el compliment.	**Responsable implantació**	Cap de seguretat
	Data prevista d'implantació	01/02/2014
	Representant de l'empresa	Jordi Miró Amigó
	Firma	

Nº Observació	OB/11	**Data**	01/12/2013
Descripció de l'observació			
Podem observar que en el que fa referència al compliment de les polítiques, i normes, així com les diferents consideracions sobre l'auditoria cal portar-los a un procés de millora contínua, aplicant totes les diferents revisions que es realitzin, tenint en compte que el procés implantat està molt desenvolupat fins el moment.		**CMM**	L4
Paràgraf de la norma	[15.]		
Nom de l'auditor	Jordi Miró Amigó	**Auditor en cap**	Jordi Miró Amigó
Firma		**Firma**	

5.8.3. Taula de resum de les no-conformitats i de les observacions:

En la següent taula de resum podem observar els totals de no-conformitats majors i menors, i les observacions detectades per l'equip auditor de cadascun dels diferents punts agrupats de la ISO.

Normativa ISO	NC Majors (CMM 0-1)	NC Menors (CMM 2-3)	Observacions (CMM 4)	Conformitat (CMM 5)
[5.] Política de seguretat.	0	1 (2 sub-apartats)	0	0
[6.] Aspectes organitzatius de la seguretat de la informació.	0	1 (8 sub-apartats)	1 (1 sub-apartat)	1 (1 sub-apartat)
[7.] Gestió d'actius.	0	1 (2 sub-apartats)	1 (3 sub-apartats)	0
[8.] Seguretat lligada als recursos humans.	0	1 (4 sub-apartats)	1 (1 sub-apartat)	1 (4 sub-apartats)
[9.] Seguretat física i de l'entorn.	0	1 (12 sub-apartats)	0	0
[10.] Gestió de comunicacions i operacions.	0	1 (14 sub-apartats)	1 (11 sub-apartats)	1 (4 sub-apartats)
[11.] Control d'accés.	0	1 (9 sub-apartats)	1 (14 sub-apartats)	0
[12.] Adquisició, desenvolupament i manteniment dels sistemes de informació.	0	1 (8 sub-apartats)	1 (1 sub-apartat)	1 (6 sub-apartats)
[13.] Gestió de incidents de seguretat de la informació.	0	0	1 (5 sub-apartats)	0
[14.] Gestió de la continuïtat del negoci.	0	1 (1 sub-apartat)	1 (4 sub-apartats)	0
[15.] Compliment.	0	1 (2 sub-apartats)	1 (5 sub-apartats)	1 (3 sub-apartats)
TOTALS:	0	10 (62 sub-apartats)	9 (45 sub-apartats)	5 (18 sub-apartats)

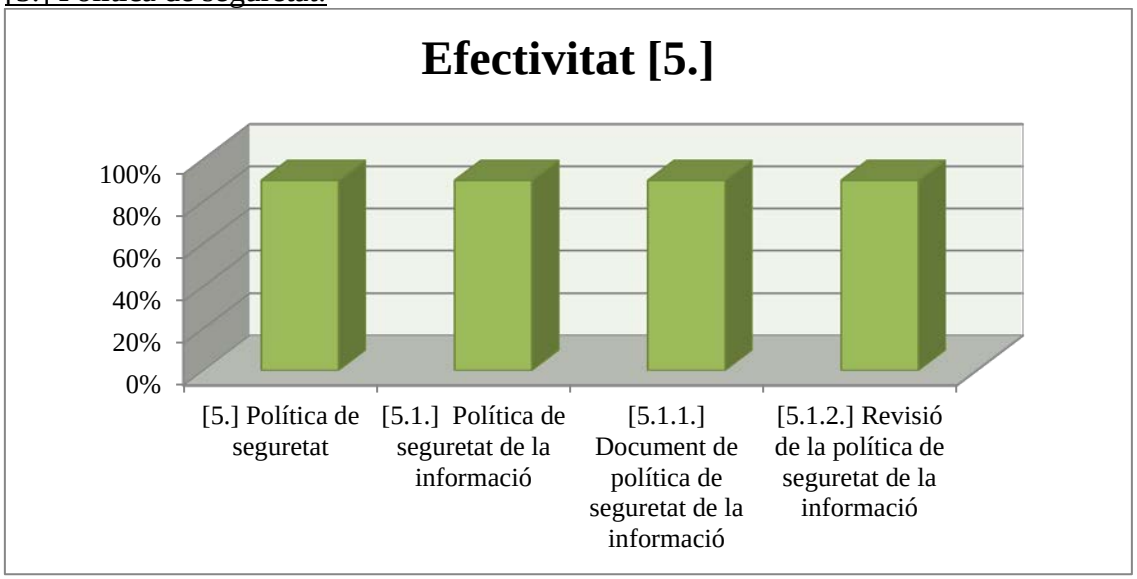
Després de realitzar el recompte de totes les no-conformitats i de les diferents observacions detectades dels diferents apartats i sub-apartats, podem destacar-ne:

- No-conformitats majors (CMM L0 i L1): 0 detectades.
- No-conformitats menors (CMM L2 i L3): 10 agrupacions de 62 sub-apartats.
- Observacions (CMM L4): 9 agrupacions de 45 sub-apartats.
- Amb conformitat, i sense observacions (CMM L5): 5 agrupacions en 18 sub-apartats.

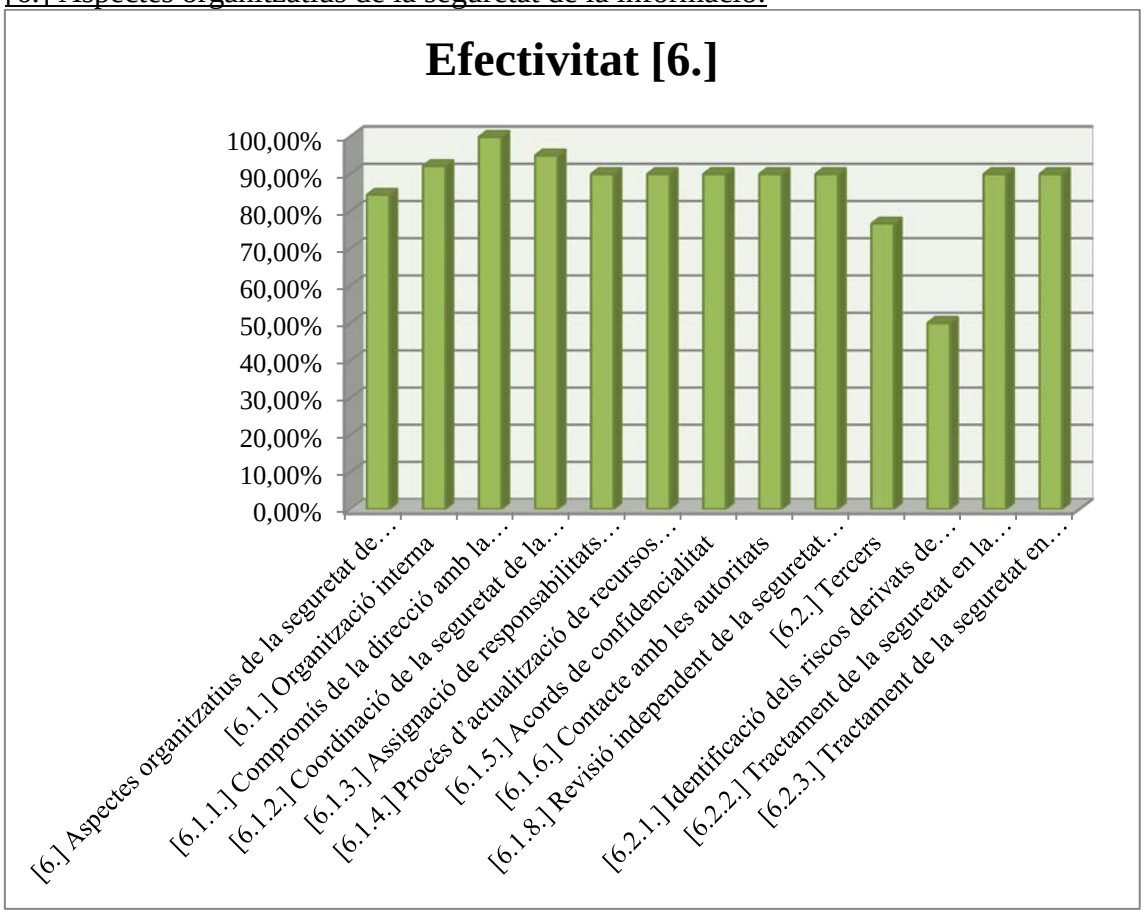
5.8.4. Diagrames de columnes de l'efectivitat dels controls ISO 27002:

En els següents diagrames de columnes podrem observar quins nivells d'efectivitat disposen els diferents controls de tot el sistema que hem de tenir en compte per certificar l'empresa a la ISO 27002.

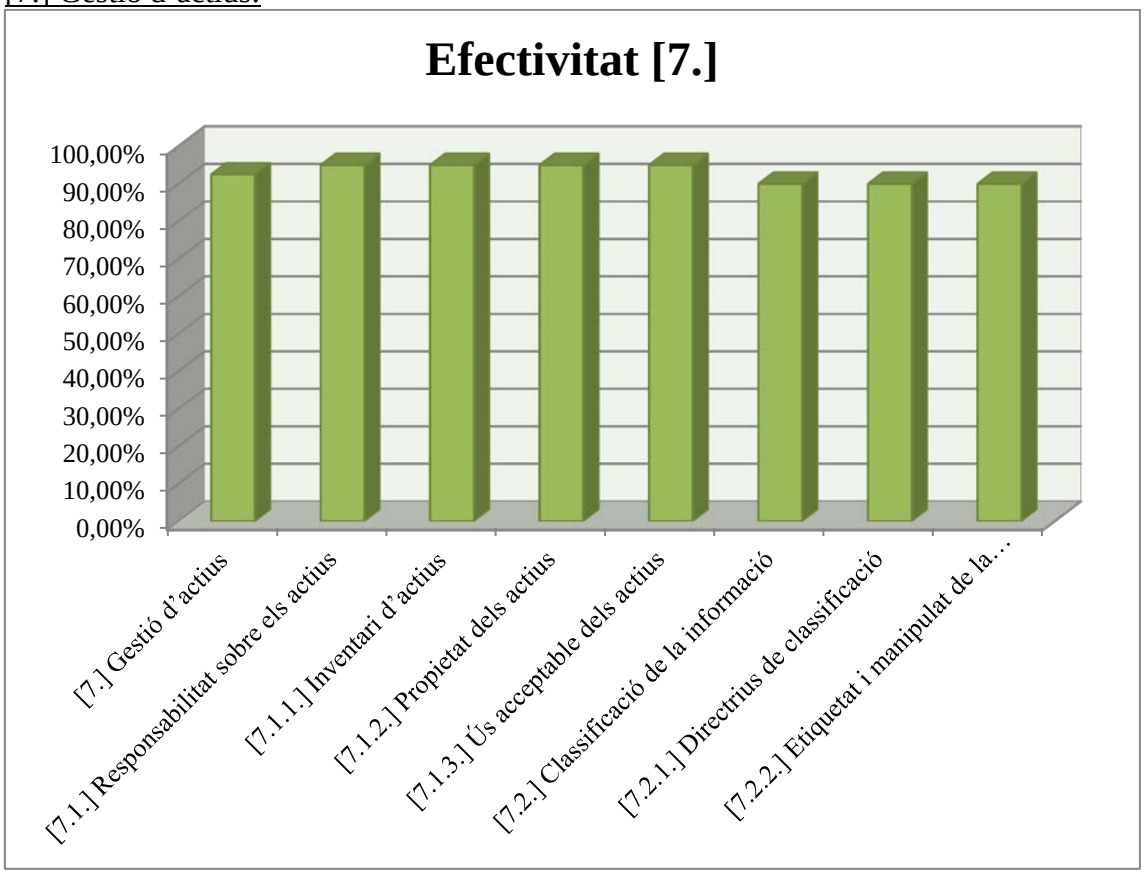
[5.] Política de seguretat:



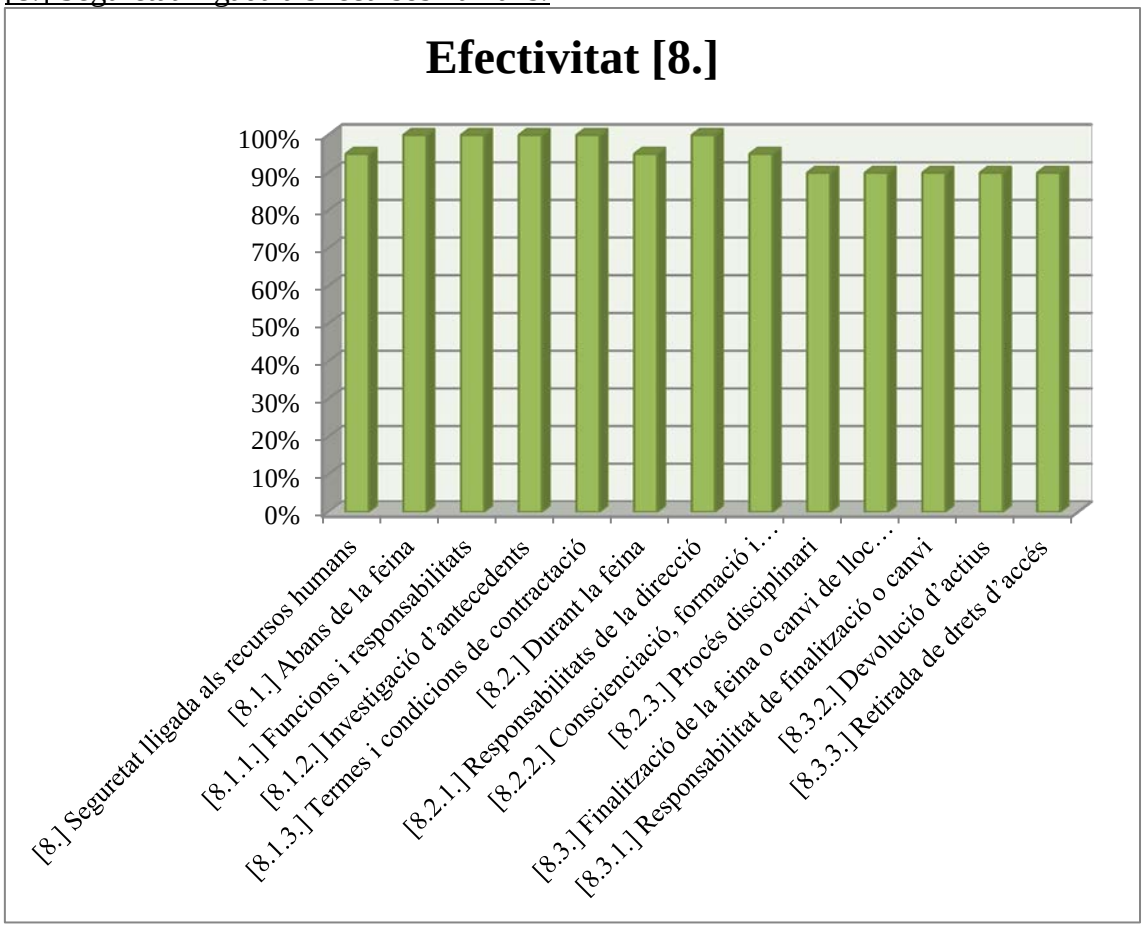
[6.] Aspectes organitzatius de la seguretat de la informació:



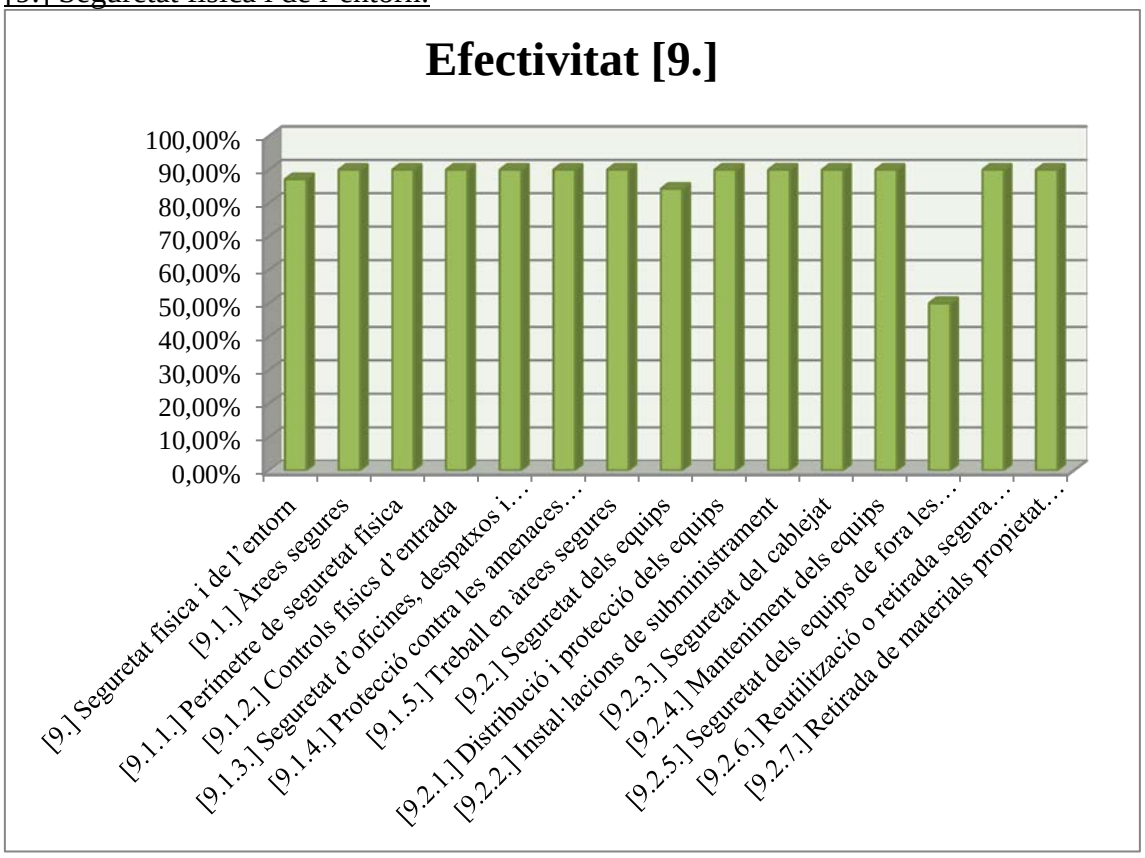
[7.] Gestió d'actius:



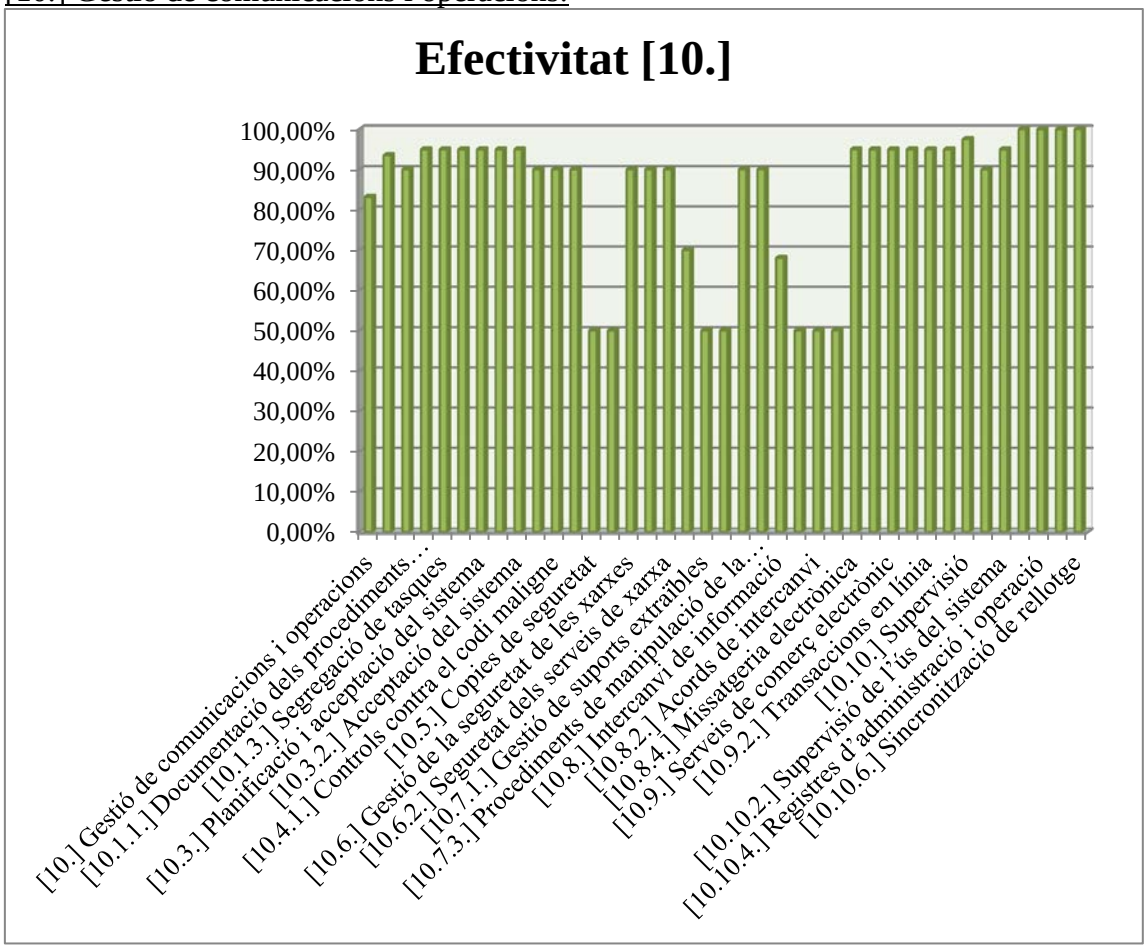
[8.] Seguretat lligada als recursos humans:



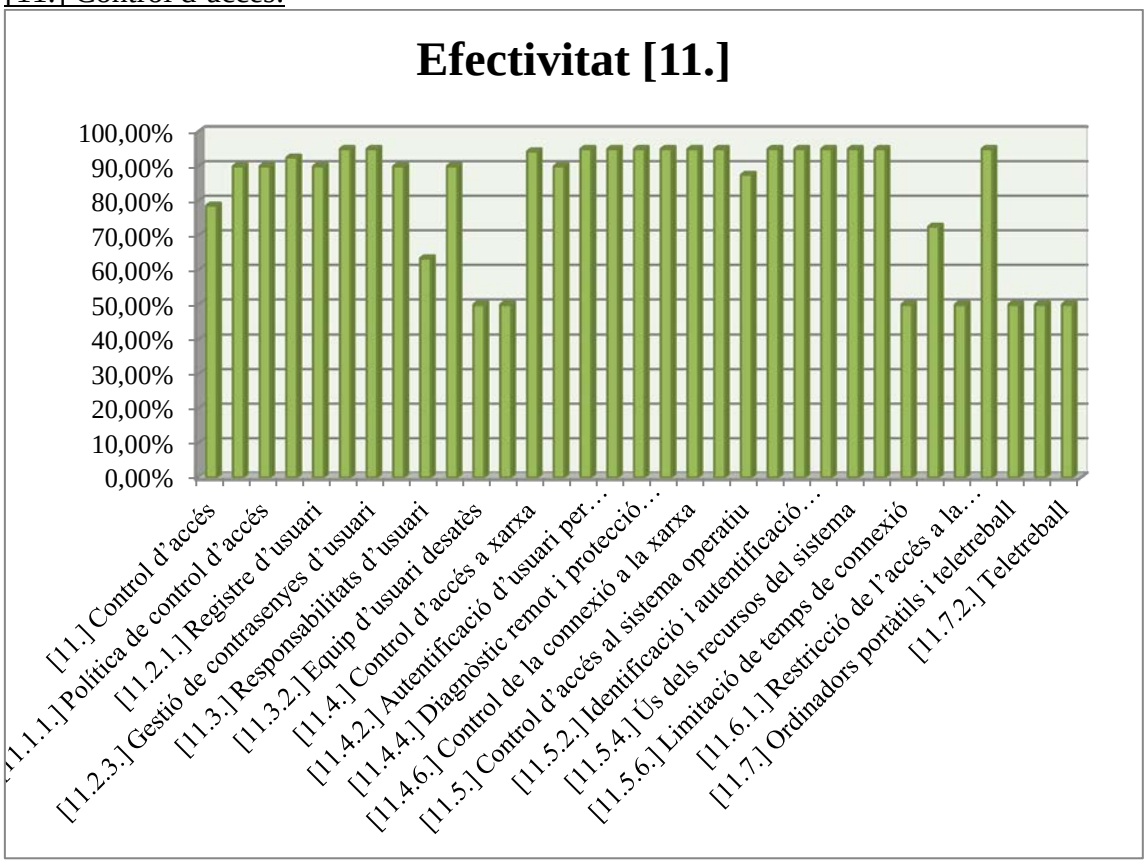
[9.] Seguretat física i de l'entorn:



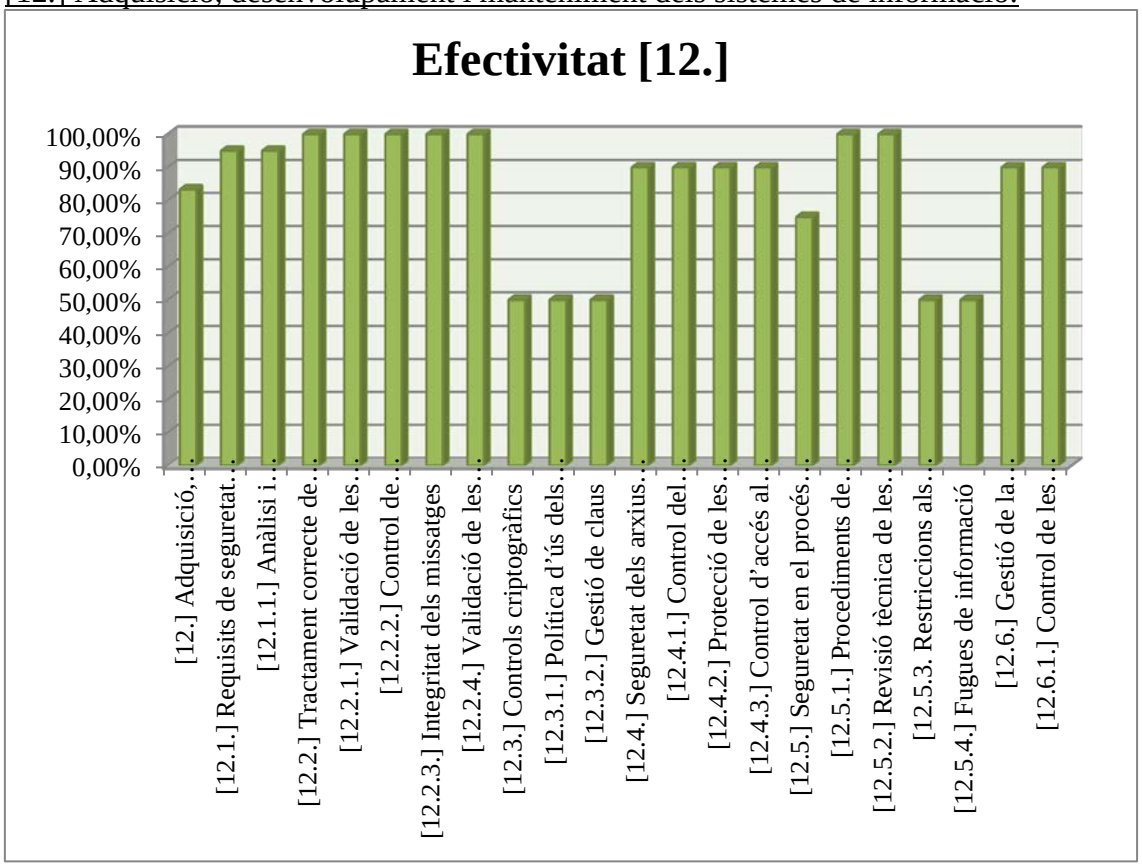
[10.] Gestió de comunicacions i operacions:



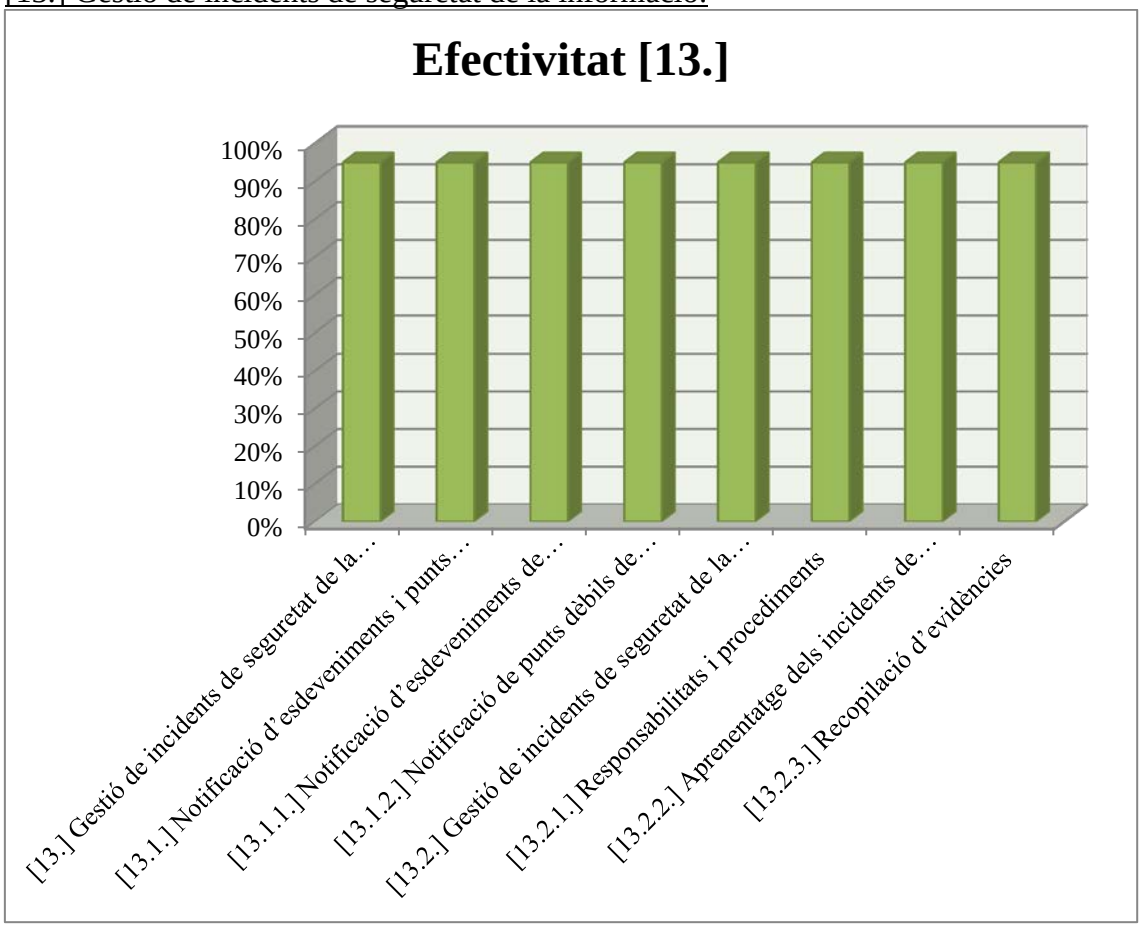
[11.] Control d'accés:



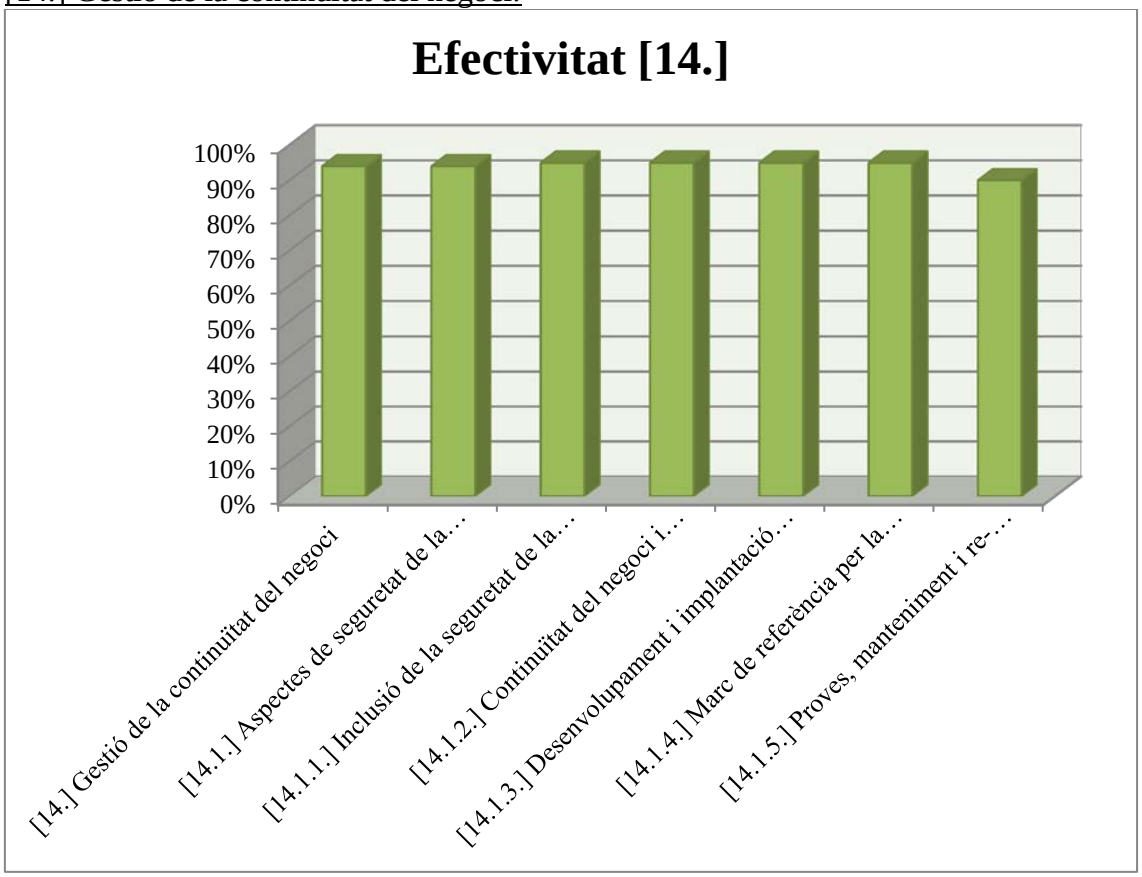
[12.] Adquisició, desenvolupament i manteniment dels sistemes de informació:



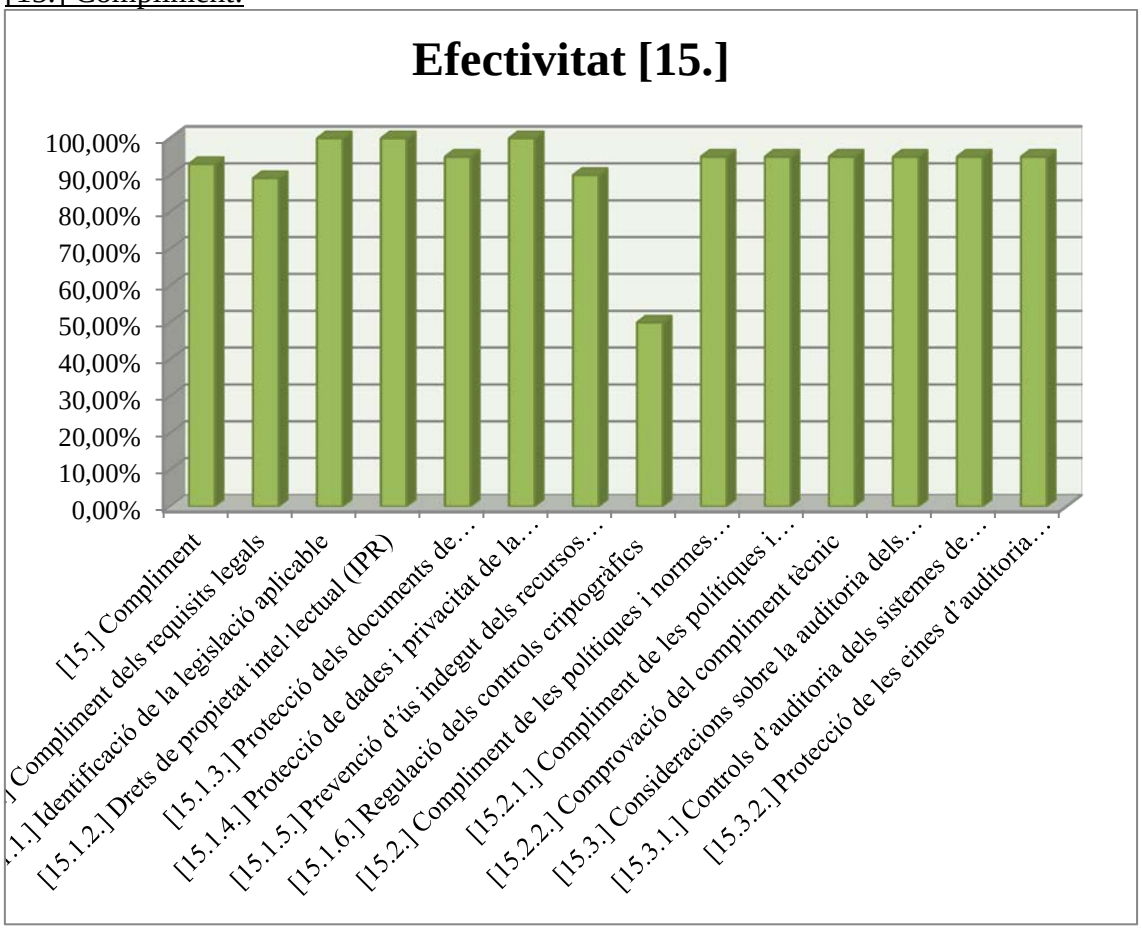
[13.] Gestió de incidents de seguretat de la informació:



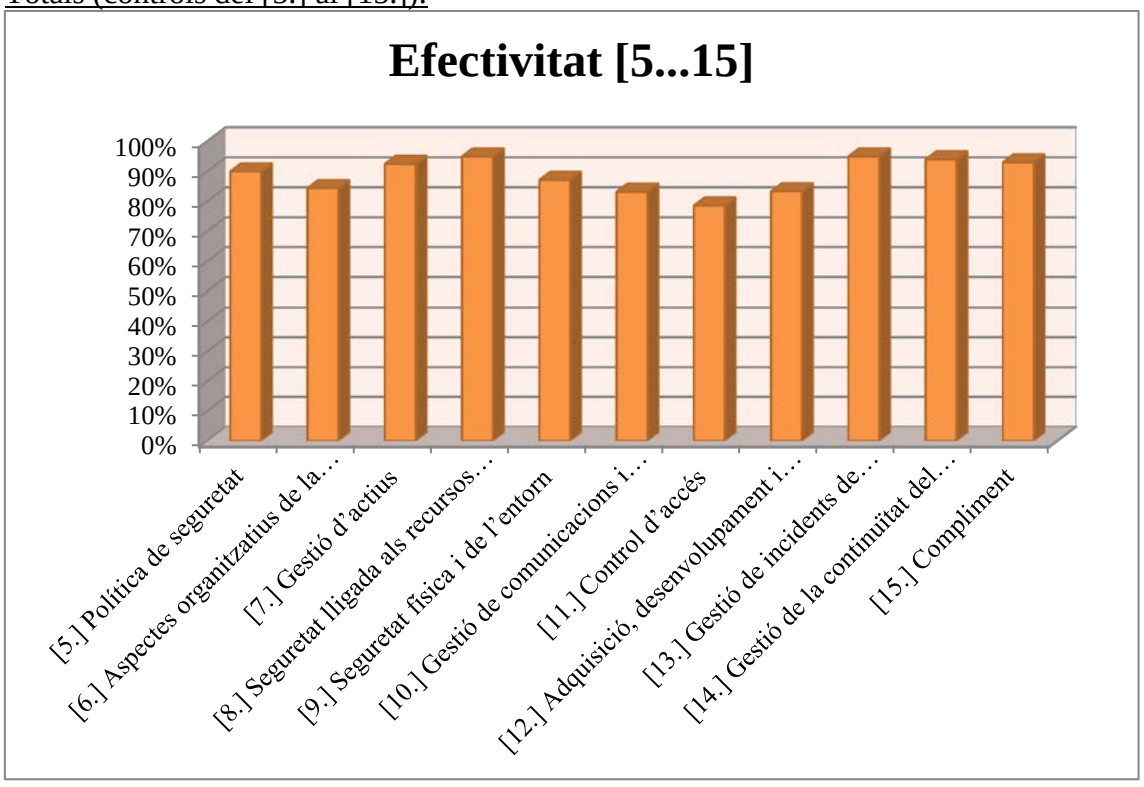
[14.] Gestió de la continuïtat del negoci:



[15.] Compliment:



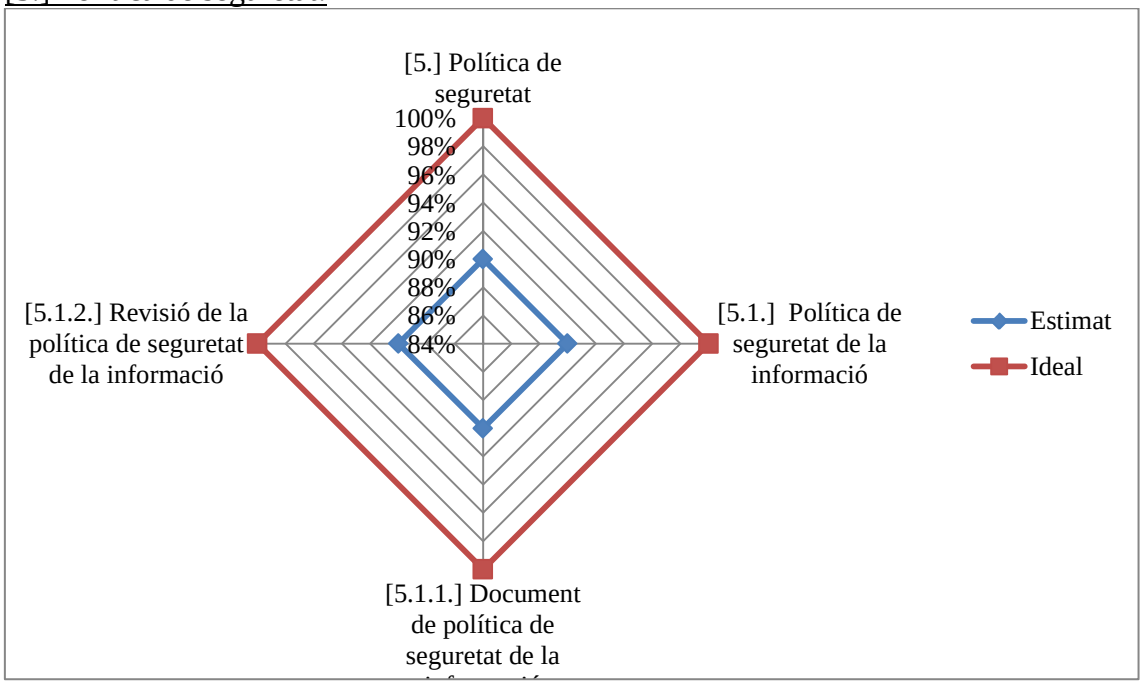
Totals (controls del [5.] al [15.]):



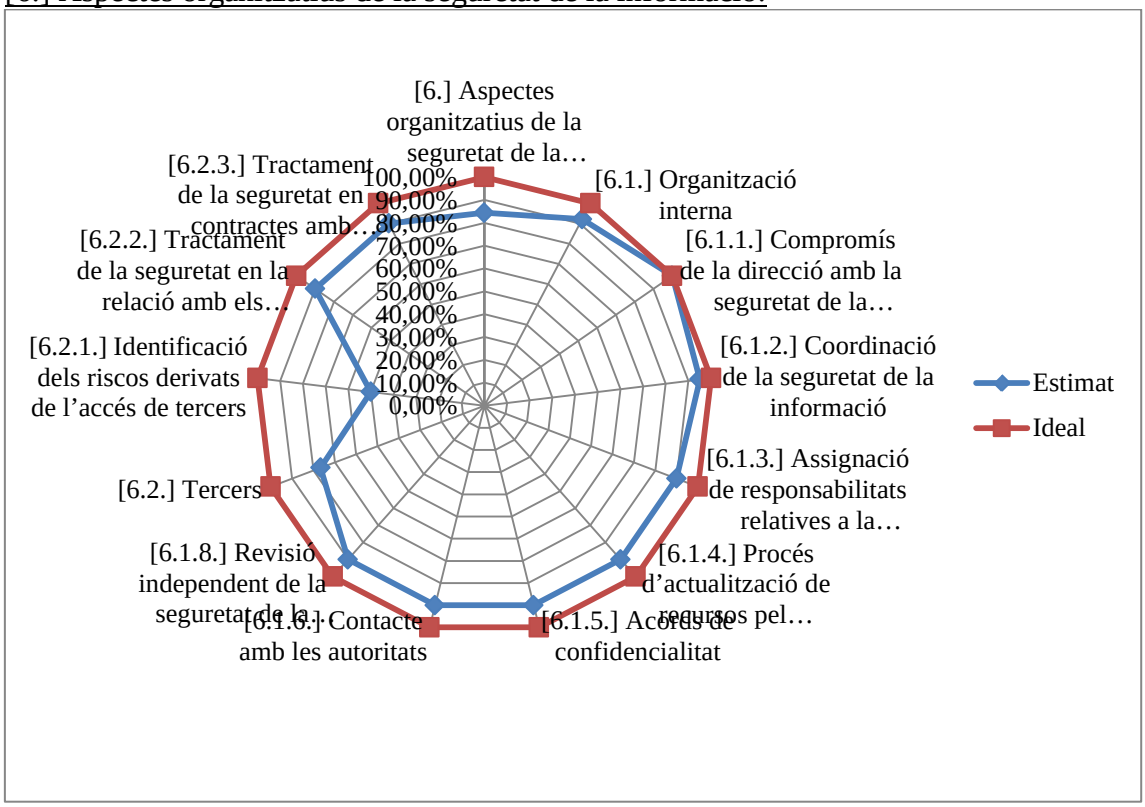
5.8.5. Diagrames de radar de l'efectivitat dels controls ISO 27002:

Tot seguit podem veure els diagrames de radar que ens permeten veure la diferencia entre el valor estimat i el valor d'un marc de seguretat ideal. Cal dir, que en els següents diagrames, i perquè es visualitzin molt millor les diferencies entre cada control, l'escala de cada diagrama de radar està personalitzada (alguns van del 0% al 100%, i d'altres, per exemple, de 84% al 100%).

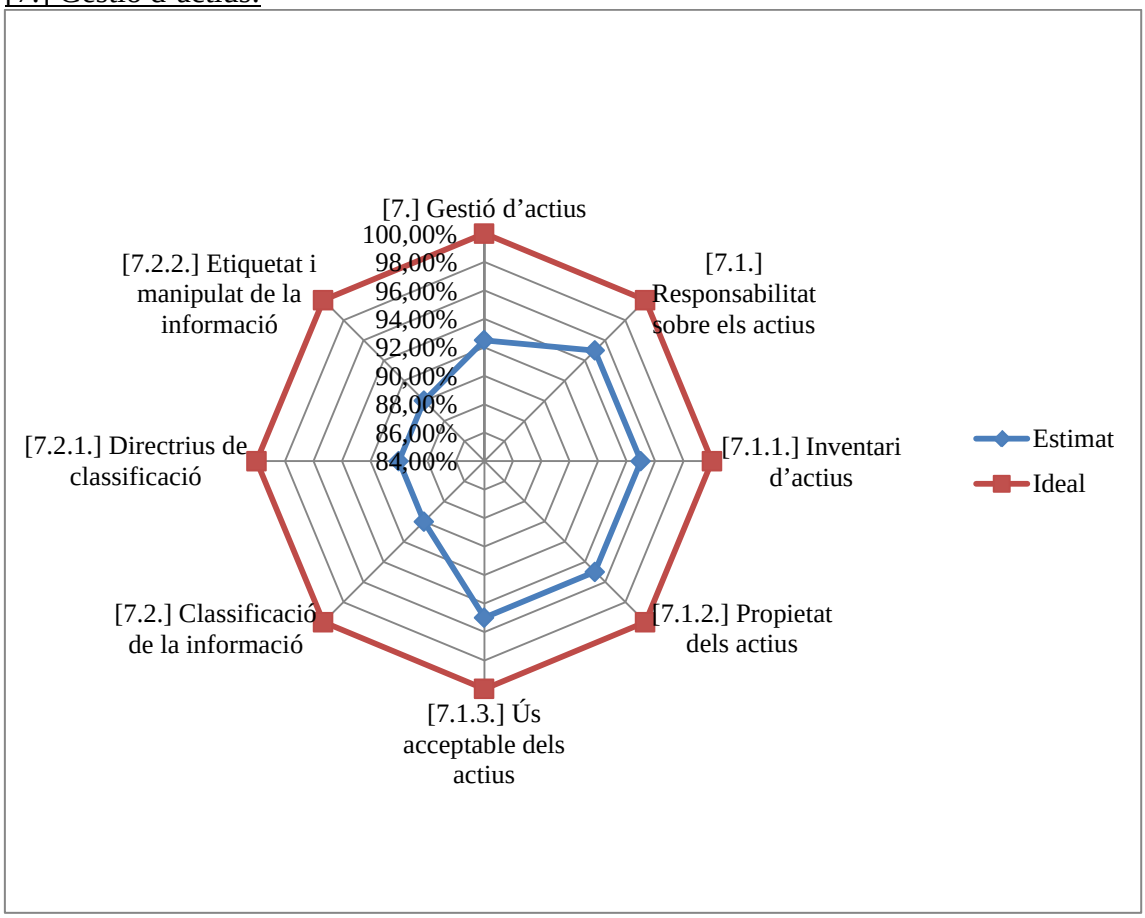
[5.] Política de seguretat:



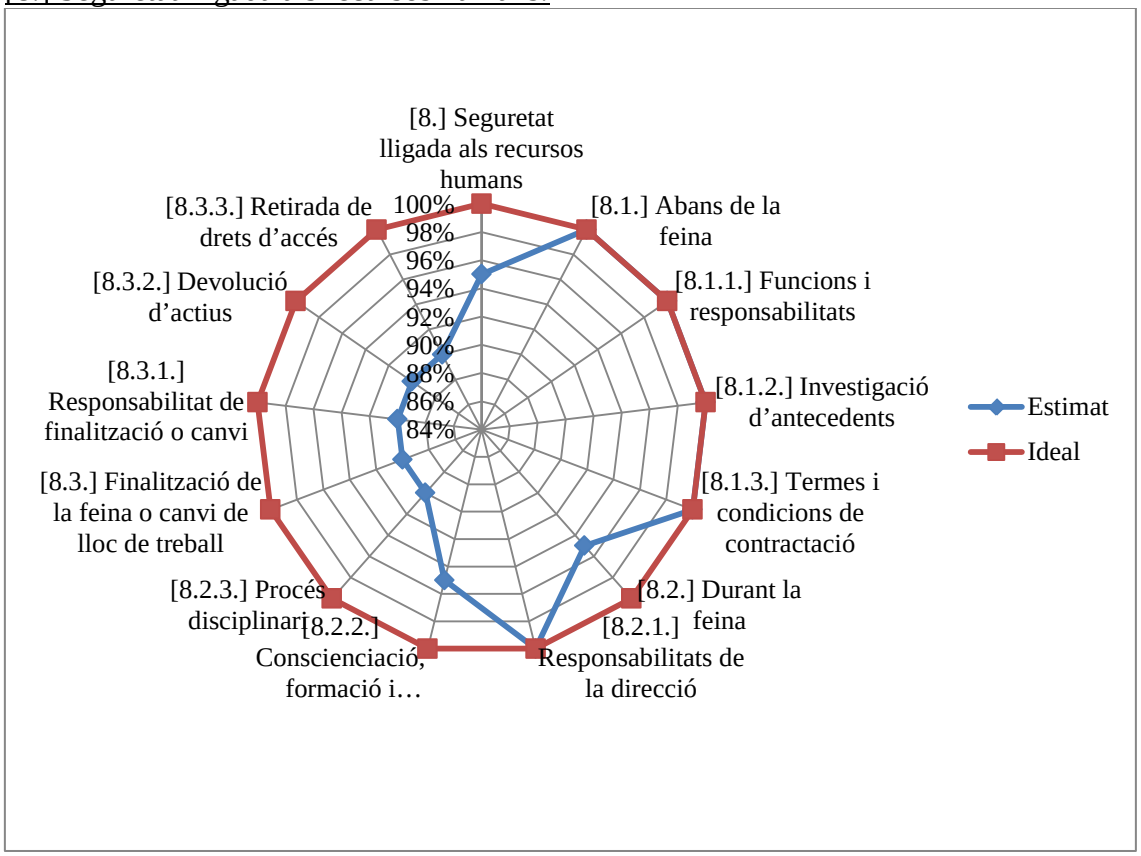
[6.] Aspectes organitzatius de la seguretat de la informació:



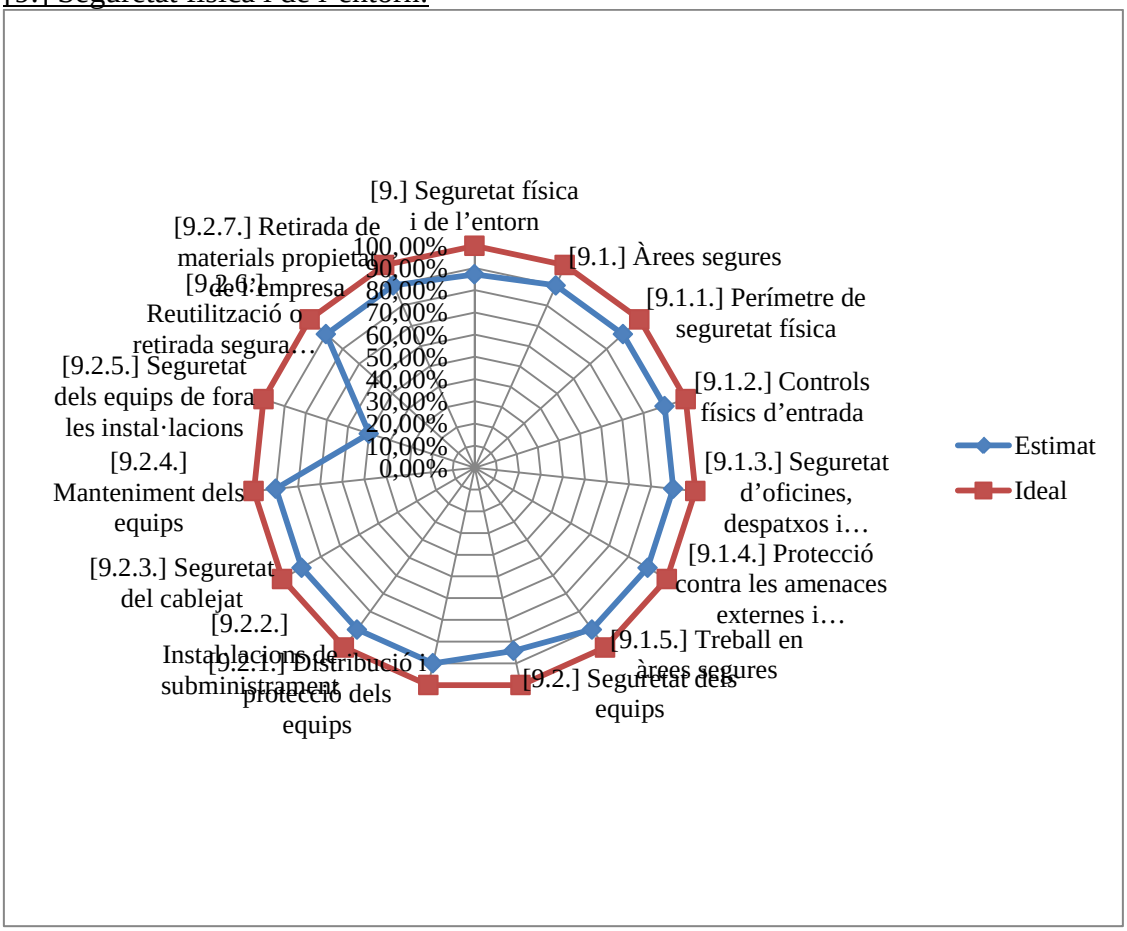
[7.] Gestió d'actius:



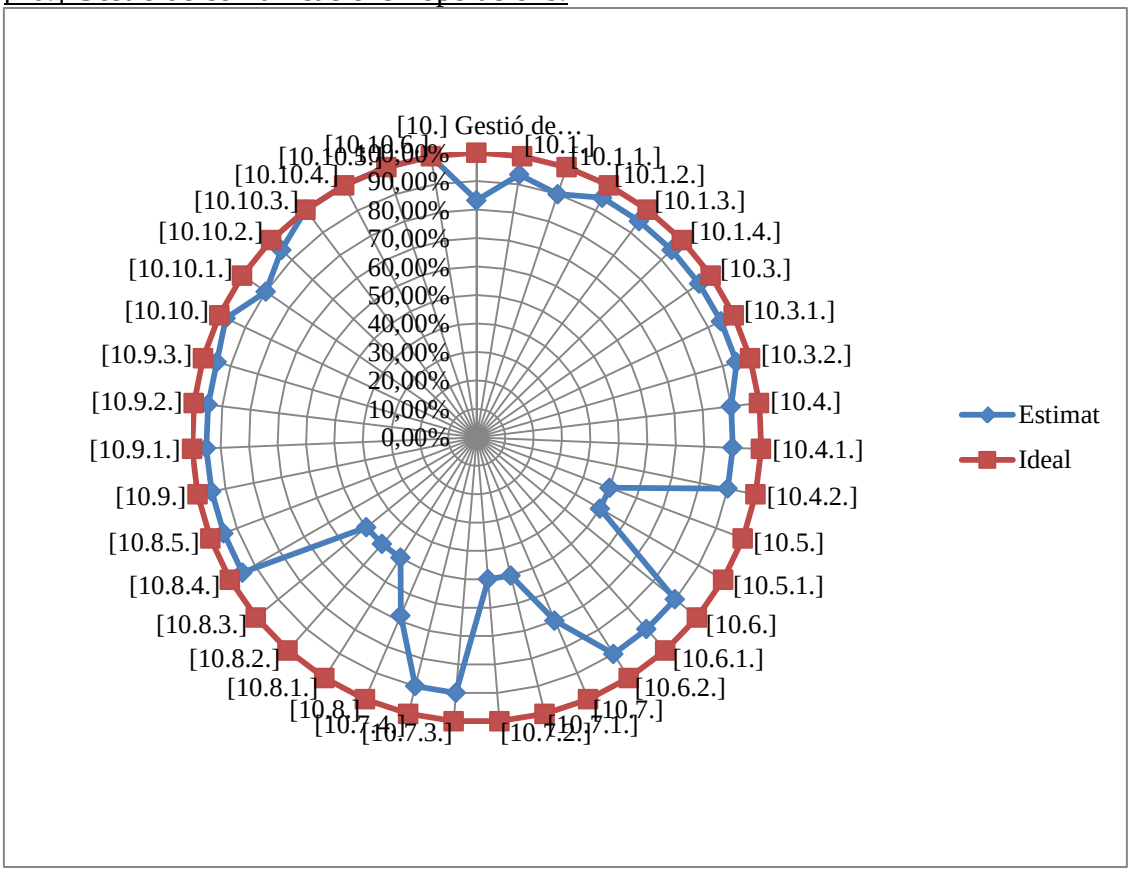
[8.] Seguretat lligada als recursos humans:



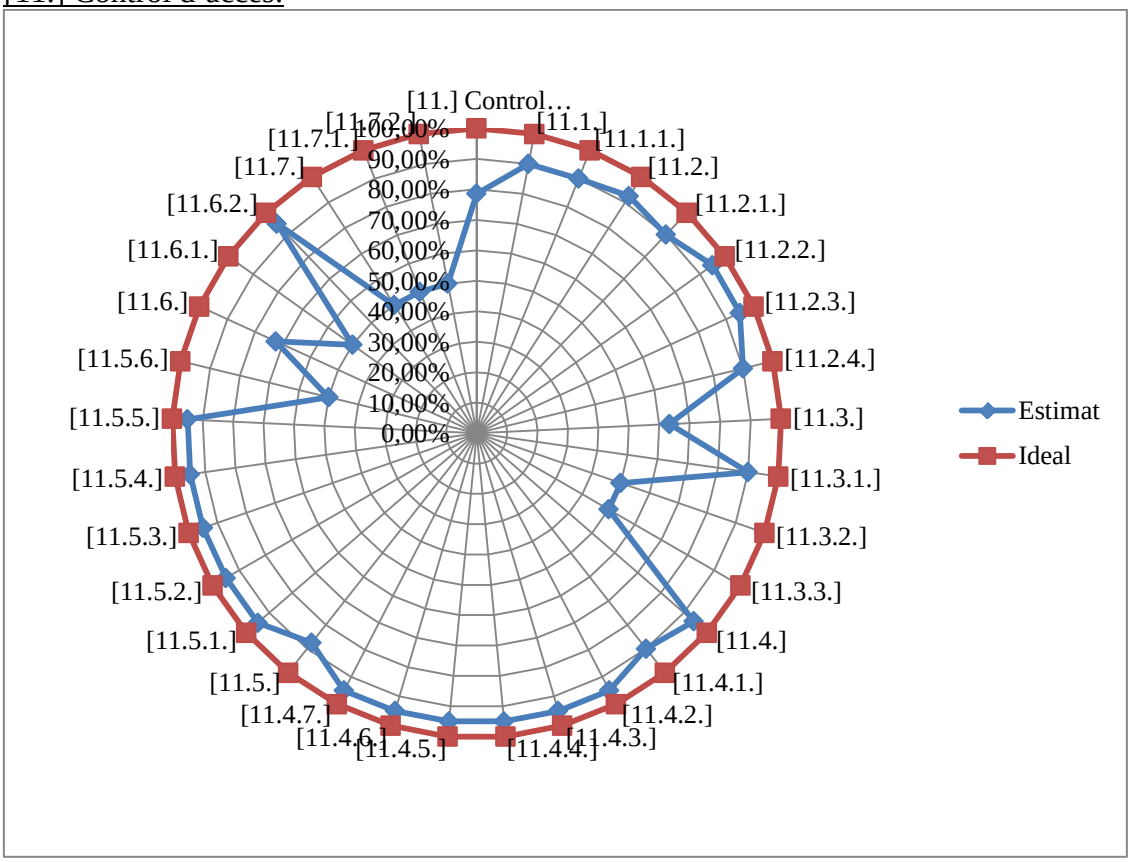
[9.] Seguretat física i de l'entorn:



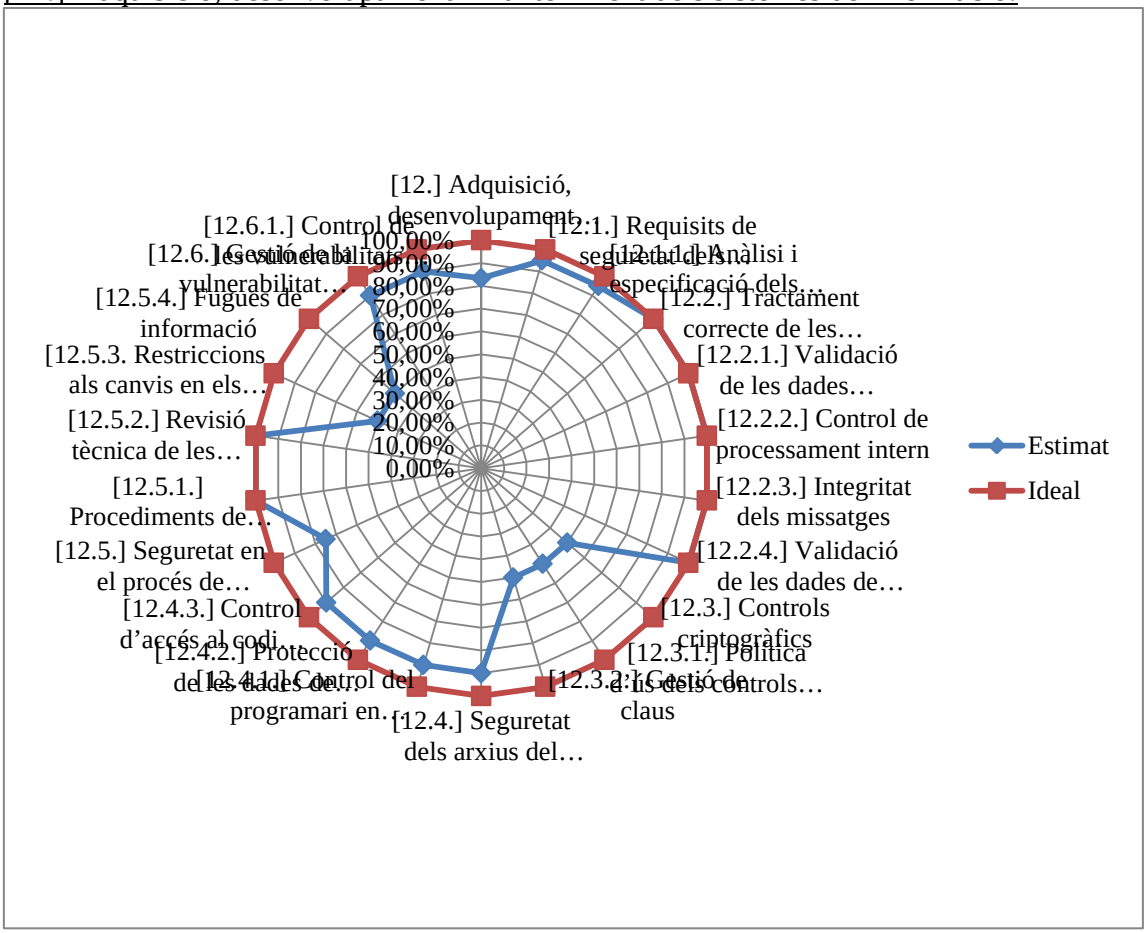
[10.] Gestió de comunicacions i operacions:



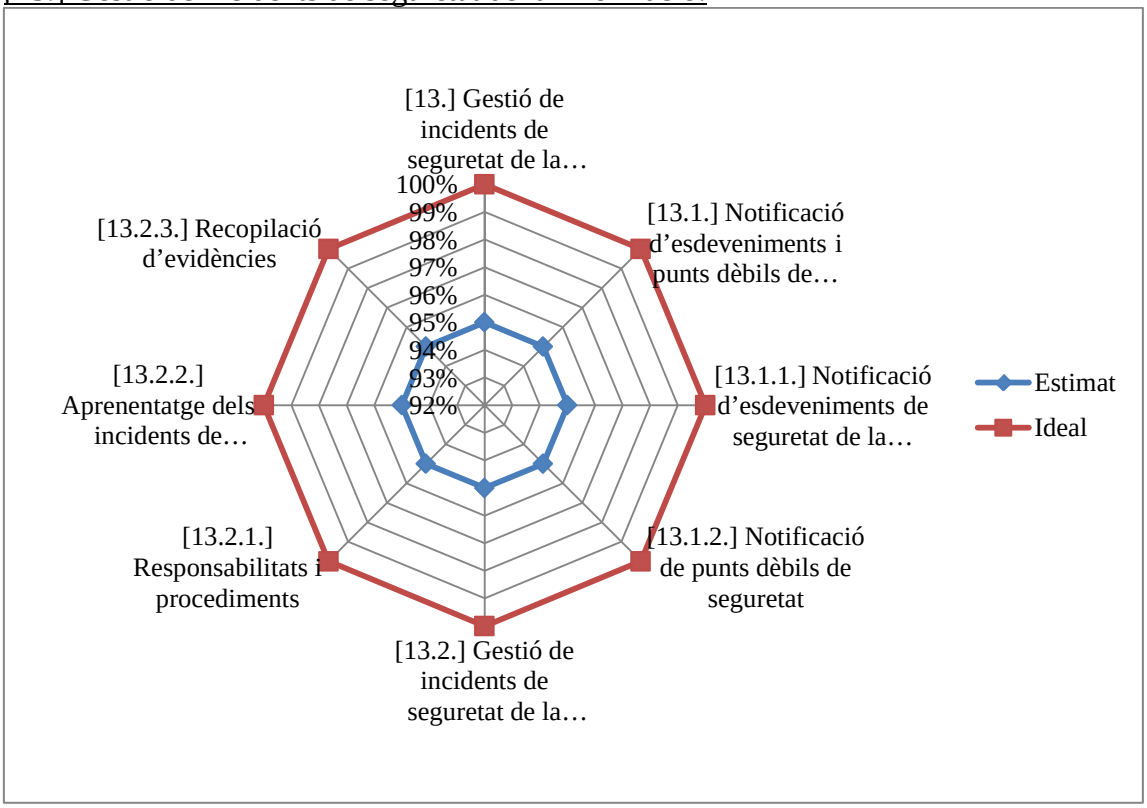
[11.] Control d'accés:



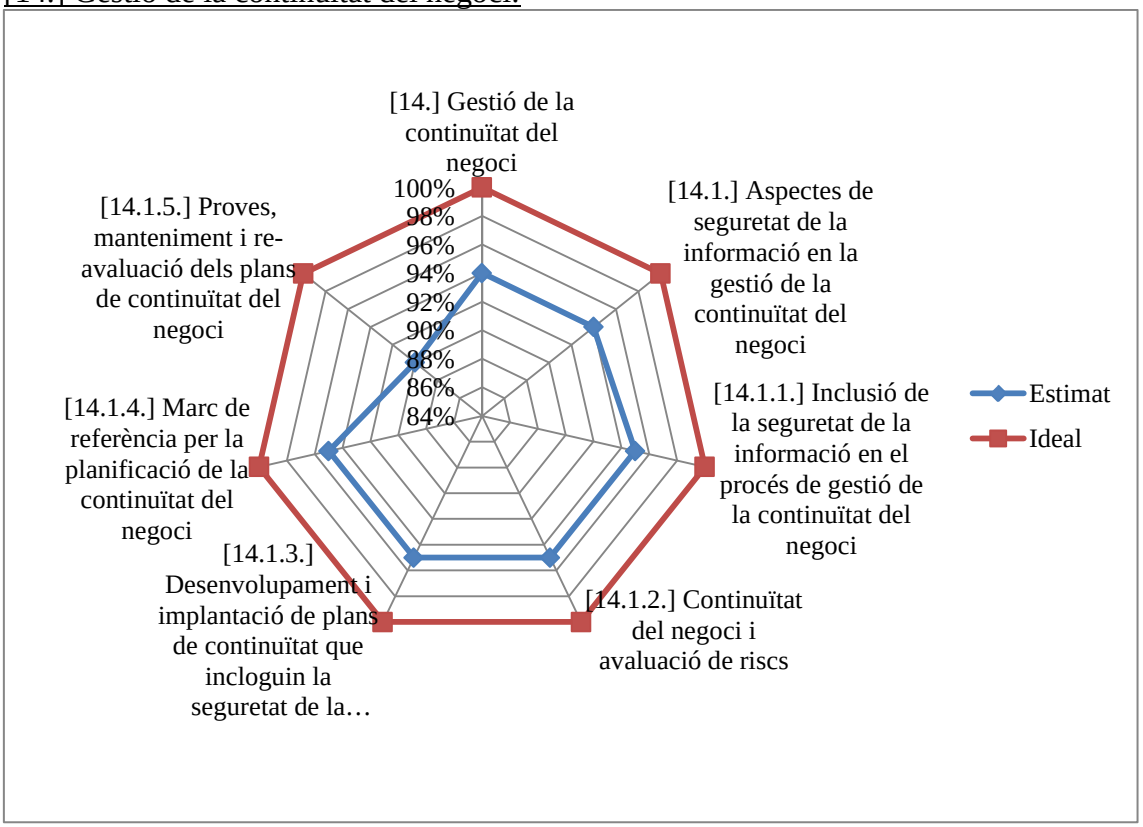
[12.] Adquisició, desenvolupament i manteniment dels sistemes de informació:



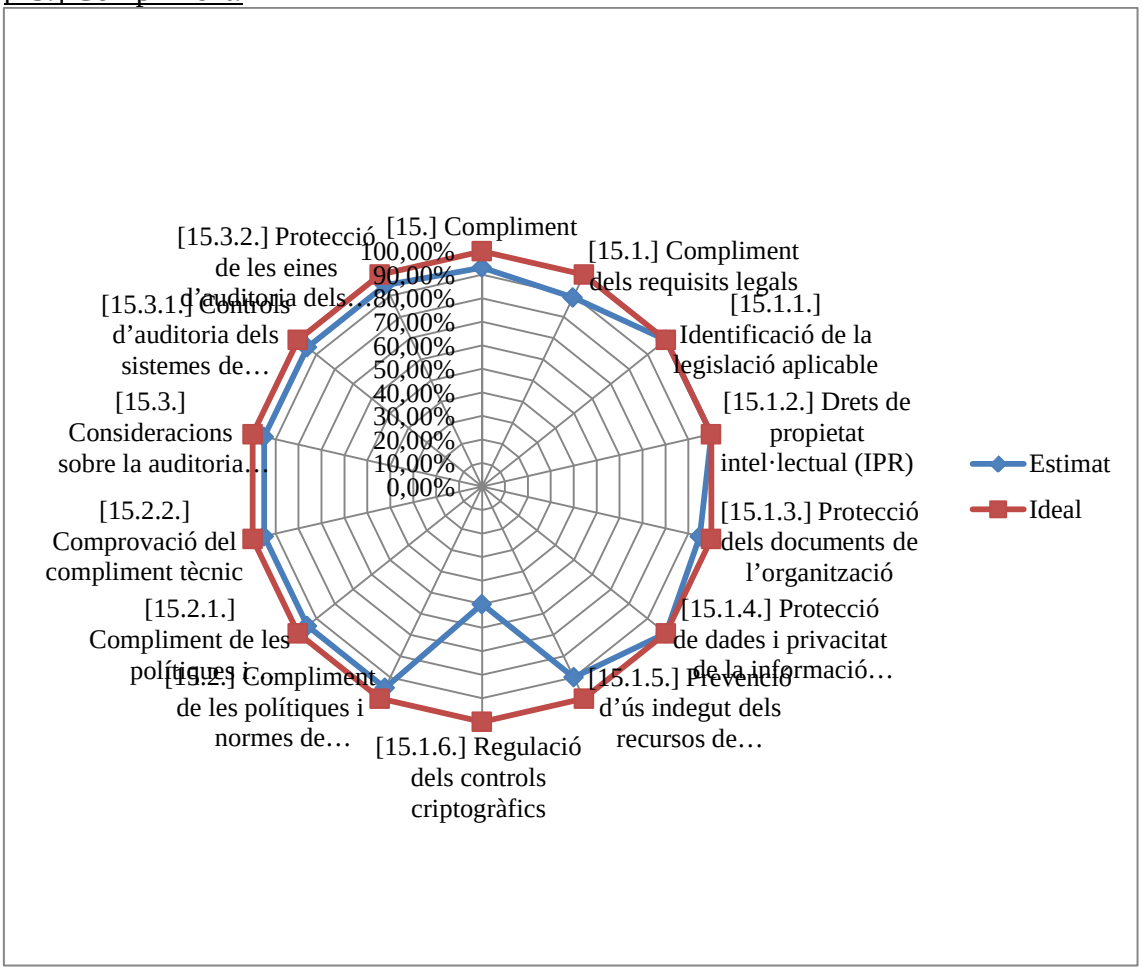
[13.] Gestió de incidents de seguretat de la informació:



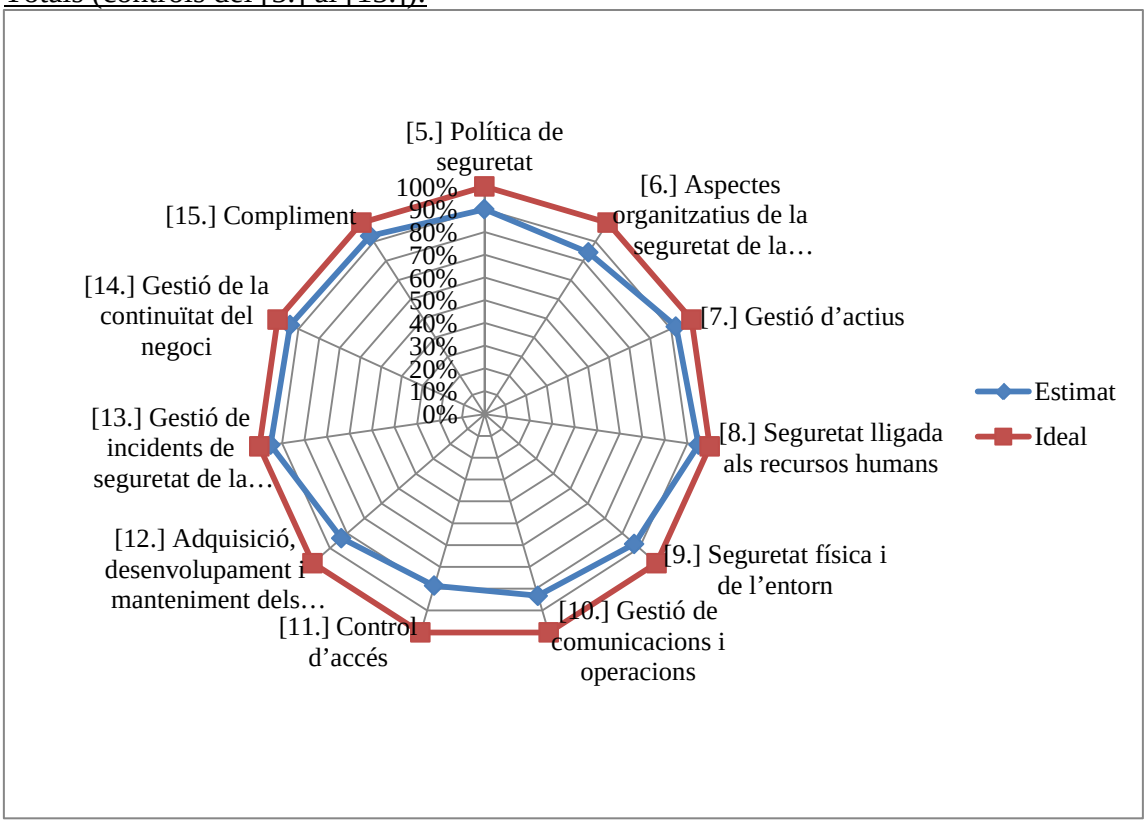
[14.] Gestió de la continuïtat del negoci:



[15.] Compliment:



Totals (controls del [5.] al [15.]):



5.8.6. Conclusions de la taula i dels diagrames de compliment:

Primerament cal dir que els valors anteriors, tant de la taula de compliment de la ISO 27002, i dels posteriors diagrames, són uns valors d'efectivitat estimada, ja que fins que no es realitzen els projectes proposats en l'empresa, i en l'entorn real d'aplicació, no és pot saber exactament la seva efectivitat real.

En segon lloc, tal i com podem observar en la taula i en els diferents diagrames, podem veure que existeix una gran efectivitat estimada després de la aplicació dels diferents projectes proposats en l'apartat anterior, el que ens fa pensar que en una posterior auditoria portada a terme per professionals externs a l'empresa, els valors objectius d'anàlisi de l'empresa seran molt similars, i que per tant, la certificació de l'empresa en la ISO 27002 serà possible.

En tercer lloc, cal dir que entre els diferents valors d'efectivitat, podem trobar controls ISO del sistema que tenen una gran efectivitat, (valors del 100%, L5), ja que es considera que són processos del sistema que es porten a terme seguint un model o metodologia optimitzat i de millora contínua.

En el terme mig, trobem elements que gràcies als projectes proposats es pot estimar que milloraran l'efectivitat a valors del 90% L3 i 95% L4.

Així com també podem observar que existeixen alguns elements que se situen a nivells d'efectivitat del 50% L2, i que en posteriors anàlisis i millores continues del sistema s'hauran de proposar millores per fer augmentar aquests nivells, i per tant, augmentar la seguretat notablement de tot el sistema de informació.

Seguint en la mateixa línia, cal dir que en el cas que l'auditoria externa posterior donés alguna disconformitat greu o lleu no detectada anteriorment, podríem solucionar-les amb els terminis adequats i assignats a cada nou projecte de millora que fos necessari, i després de l'acceptació i portada a terme la millora, podríem tornar a sotmetre a auditoria el sistema d'informació de l'empresa, per poder arribar a certificar-la adequadament i portar l'empresa a un procés imprescindible, ideal i de millora contínua de la seguretat de tota la infraestructura i dels sistemes de l'empresa.

6. Conclusions finals del projecte:

Com a conclusions finals del projecte es pot comentar que mitjançant l'elaboració d'aquest projecte s'ha pogut observar la situació de l'empresa, amb els diferents riscos i amenaces a les que es troba exposada la mateixa, així com també s'ha pogut observar els projectes que podríem implantar i finalment s'ha pogut analitzar el nivell actual de compliment de l'organització amb referencia amb la normativa ISO 27002.

Així mateix, amb la realització d'aquest projecte, l'empresa disposa d'un document de referència amb el que centrar els seus esforços de seguretat de la informació. Evidentment, és un document inicial, i que haurà d'evolucionar i anar millorant cíclicament per poder incorporar nous plans d'acció per noves situacions de risc a que pot estar exposada l'empresa en un futur o per canvis de la infraestructura o dels processos productius de l'organització.

Hem de tenir clar que sempre els plans d'acció o projectes proposats hauran de cercar l'objectiu de minimitzar les possibles amenaces i reduir el risc a que estaran sotmesos els diferents actius, i per tant, reduir una possible materialització de l'amenaça. I un punt clau en aquest aspecte és els plans de continuïtat del negoci. Així mateix tots aquests elements ens permetran assegurar el compliment de la normativa ISO, i alhora el compliment de la normativa legal vigent.

Els diferents programes i projectes a aplicar hauran de realitzar una gestió de prevenció de possibles incidències per poder detectar-les i prevenir-les abans que es materialitzin, així com també s'han de disposar de programes que ens permetin reaccionar ràpidament en el cas que es produeixi una incidència que no teníem controlada, i aturar la materialització de danys eficientment, o també es pot donar el cas, que el cost de controlar-la era tant alt que era millor assumir-lo com a risc o cedir el risc a terceres organitzacions, per exemple, mitjançant la contractació d'una assegurança externa.

Per tant, ho podem resumir amb:

- És imprescindible la seguretat per tots els elements de la infraestructura de l'empresa, i elements relacionats.
- L'actualització constant i ús de noves tecnologies és bàsica.
- Per complir la normativa legal hem de poder tenir controlada la seguretat del nostre sistema.
- Hem de poder fer front a incidències no detectades amb plans de continuïtat del negoci.
- Una bona seguretat fa el negoci més eficient.
- Cal una formació continuada dels empleats.
- És imprescindible el compromís de direcció.
- Hem de controlar el risc segons el cost, i la criticitat dels nostres sistemes.

- S'ha de millorar contínuament (PDCA).

Algunes de les tasques que s'hauran de realitzar en l'oficina de seguretat de l'empresa, i concretament amb el responsable de seguretat en un futur, són les següents:

- Seguir implementant controls, i mantenir actualitzat l'inventari d'actius i l'anàlisi de riscos.

- Disposar d'una documentació sempre actualitzada, revisada i degudament publicada, perquè tots els membres la respectin i la compleixin.

- Disposar d'una monitorització dels diferents elements de xarxa i dels diferents actius que puguin ser problemàtics o essencials en un present o futur.

- Conscienciar els empleats que és important mantenir una correcta seguretat en els seus llocs de treball, i amb els arxius i documents que manipulin.

- Disposar, sempre que el pressupost sigui el suficient, de totes les millores i actualitzacions de maquinari, programari, elements de xarxa, o eines d'encriptació, que ens permetin assegurar les diferents dimensions de seguretat comentades en el projecte.

- Disposar de proves i realitzar auditories internes i externes periòdicament per tal d'assegurar que la seguretat del sistema és l'òptima

Per finalitzar cal dir que l'elaboració d'aquest projecte, ha permès observar de forma detallada totes les diferents fases d'elaboració d'un pla, i que ens ha permès observar la forma correcte la realització d'un inventari d'actius, l'anàlisi de riscos, l'anàlisi d'amenaces, els riscos, i quins projectes proposats poden ajudar-nos en la nostre organització per millorar-ne la seguretat, i per últim s'ha pogut comprovar quin és el nivell de compliment amb una auditoria interna de la normativa ISO, per assegurar-nos que en una possible auditoria externa de certificació els resultats serien els més satisfactoris.

7.Bibliografia:

En aquest projecte s'han utilitzat els següents recursos, per a portar a terme les diferents seccions o apartats:

- **Recursos electrònics:**

- Metodologia MAGERIT: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Uk1Ai4a-2m4

- Document ISO 17799: http://www.17799.com/papers/iso17799scope.pdf

- Traducció al castellà de la norma ISO 17799: http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

- LOPDP (Agencia Espanyola de Protecció de Dades): http://www.agpd.es

- Informació ISO 27001 i ISO 27002: http://www.iso27000.es

- Informació SGSI (Inteco): http://www.inteco.es

- **Apunts:**

- Apunts i coneixements adquirits del màster que he cursat, Màster Oficial de Programari Lliure UOC.

- Apunts i coneixements adquirits del màster que he cursat, Màster Oficial de Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC – UOC, UAB, URV, UiB).

8.Evolució i versions del projecte:

En el següent requadre podem veure l'evolució dels diferents apartats del projecte:

Identificació:			
Autor: Jordi Miró Amigó		**Projecte:** TFM MISTIC.	
Data d'inici del projecte: Setembre 2013		**Data del final del projecte:** Gener 2014	
Modificacions del projecte (versions):			
Índex del projecte	**Versió**	**Data de creació**	**Data última revisió**
FASE I (Introducció)	2.0	Octubre de 2013	Novembre de 2013
FASE II (Documentació)	2.0	Octubre de 2013	Novembre de 2013
FASE III (Anàlisis de riscos)	2.0	Novembre de 2013	Desembre de 2013
FASE IV (Propostes projectes)	2.0	Novembre de 2013	Desembre de 2013
FASE V (Audit. compliment)	2.0	Desembre de 2013	Desembre de 2013
FASE VI (Memòria final)	2.0	Desembre de 2013	Gener de 2014
Resum executiu	2.0	Desembre de 2013	Gener de 2014
Presentació del projecte	2.0	Desembre de 2013	Gener de 2014
	...		
	...		