Implementació d'un pla director de seguretat per l'Empresa XX basat en la ISO/IEC 27001:2013

Nom Estudiant: Esteban Sardañés Lobato

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

Nom Consultor: Arsenio Tortajada

Centre: UOC

Data Lliurament: 10 de Juny de 2015

FITXA DEL TREBALL FINAL

Títol del treball:	*Implementació d'un pla director de seguretat per l'Empresa XX basat en la ISO/IEC 27001:2013*
Nom de l'autor:	*Esteban Sardañés Lobato*
Nom del consultor:	*Arsenio Tortajada*
Data de lliurament (mm/aaaa):	*06/2015*
Àrea del Treball Final:	*Sistemes de Gestió de la Seguretat*
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

Aquest projecte és la part final del màster interuniversitari en Seguretat de les Tecnologies de la Informació i la Comunicació i pretén ser una execució dels coneixements adquirits durant el curs a un entorn real.

El projecte es basa en la implementació d'un pla director a una empresa real, on es vol oferir als clients un servei segur i amb alta disponibilitat i amb el temps adquirir la certificació ISO 27001:2013.

El projecte pretén trobar les principals amenaces de seguretat per l'empresa i poder implementar una sèrie de projectes i procediments per tal de millorar-ho.

Actualment no hi ha cap metodologia aplicada i el personal no està gaire conscienciat amb el factor de la seguretat informàtica.

La direcció de l'empresa considera que per poder créixer i ampliar el negoci, s'han d'assentar les bases de la seguretat de la informació, ja que és l'actiu principal amb el que es basa el negoci, per poder fer front a futurs contratemps i amenaces.

La finalitat és poder implementar els estàndards en seguretat per tal de reduir els riscos i establir els procediments d'actuació. També es pretén obtenir una metodologia proactiva que permeti anar millorant constantment.

Abstract (in English, 250 words or less):

This project is the final part of the interuniversity master's degree in Security of Information and Communications Technology and aims to be an implementation of the acquired knowledge during the course, in a real environment.

The project is based on the implementation of a security plan for a real company, which wants to offer a secure and high availability service. Over time would like to get the ISO 27001:2013.

The project aims to find the main security threats for the company and implement a series of projects and procedures in order to improve it.

Nowadays there isn't methodology in used and the staff is not very conscious of the factor of security.

The company management believes, that in order to grow and expand the business, they should to improve information security, because is the main asset based business.

The purpose about this project is to implement security standards in order to reduce risks and to establish operating procedures. It also aims to get a proactive methodology that allows to improve constantly.

Paraules clau (entre 4 i 8):

Seguretat, SGSI, Pla Director, ISO, 27001:2013

Índex

1. Introducció

1.1 Context i justificació del Treball

La importància que té la informació per les empreses a dia d'avui, és la principal motivació per dur a terme un pla director de seguretat. L'empresa sobre la que es realitzarà aquest pla, és una empresa dedicada als serveis TIC i la qual ofereix serveis de gestió, emmagatzematge i administració dels sistemes d'informació als seus clients.

L'empresa es troba en una fase de creixement i comença a treballar amb clients molt importants. Els mecanismes de funcionament enfront a la seguretat informàtica que s'utilitzen a dia d'avui a l'empresa, són els que implementa cada membre del personal amb la supervisió de l'administrador. Aquests mecanismes no estan ni definits, ni documentats, ni controlats, i amb el pla director es vol aconseguir controlar tots els processos per tal de que ajudin a millorar la seguretat i a garantir una disponibilitat en el servei.

Fins ara, els clients només contractaven alguns serveis o externalitzaven una part de la informació. Ara, l'empresa comença a créixer i a buscar noves vies de negoci. En les noves vies de negoci de l'empresa, es pretén que la majoria de clients externalitzin tota la infraestructura, i per tant, tenen tots els sistemes i tota la informació.

A part de la pròpia seguretat i la dels seus clients, l'empresa vol aprofitar aquesta implementació per poder obtenir la certificació i d'aquesta manera tenir un factor diferencial enfront a altres empreses de la seva competència, podent garantir serveis redundats i d'alta disponibilitat i un entorn segur per emmagatzemar les dades.

1.2 Objectius del Treball

L'objectiu principal del treball, és implementar un pla de seguretat per l'empresa, que ajudi a millorar la seguretat de la informació que gestiona. Tal com s'ha comentat en el punt anterior, l'empresa està creixent i adquirint unes dimensions que obliguen a portar un control i una bona gestió enfront a la seguretat de la informació pròpia i la dels seus clients.

Per dur a terme aquest pla es basarà el projecte en la ISO/IEC 27001:2013, la qual aplica uns controls de seguretat que redueixen el risc i ajuden a millorar la disponibilitat.

En el treball els principals objectius seran:

- Realitzar un anàlisi de la situació actual de l'empresa enfront a la seguretat de la informació

- Desenvolupament de la gestió documental del SGSI a implementar.
- Realització de l'Anàlisi de riscos per tal d'identificar les amenaces a les que està exposada l'empresa.
- Definició i implantació de projectes per tal de millorar la seguretat.
- Realització d'una auditoria de compliment per veure l'estat de la seguretat de la informació un cop implementats els projectes.

1.3 Enfocament i mètode seguit

A dia d'avui l'empresa no compta amb cap mecanisme per tal de gestionar la seguretat de la informació de l'empresa.

El plantejament del projecte serà per tant, establir les bases d'un pla director de seguretat basat en un model de millora continuada PDCA. El model PDCA consteix en un procés iteratiu per tal de aplicar una millora constant. Es divideix en quatre fases:

- Plan: Planificar els processos i els objectius per millorar
- Do: Aplicar i implementar aquests processos
- Check: Monitoritzar i mesurar els processos per veure quin resultat estan donant
- Act: Analitzar els processos que no s'estan complint per tal de trobar una solució o per millorar-los.

Per tal de desenvolupar el SGSI, ens centrarem en l'aplicació de la ISO/IEC 27001:2013 i en el codi de bones pràctiques ISO/IEC 27002:2013.

També aplicarem la metodologia MAGERIT en les fases del projecte.

1.4 Planificació del Treball

La planificació d'aquest projecte s'ha realitzat en sis fases.

Fase	Descripció	Data
1	Situació actual	06/03/2015
2	Sistema Gestió Documental	27/03/2015
3	Anàlisis de Riscos	24/04/2015
4	Proposta de Projectes	15/05/2015
5	Auditoria de Compliment	29/05/2015
6	Presentació de resultats	10/06/2015

2. Situació actual

2.1 Contextualització

2.1.1 Descripció Empresa

Activitat

L'empresa de la qual es realitzarà el pla director (d'ara en endavant, "Empresa XX") centra la seva activitat en el sector de les TIC.

Actualment té 20 empleats de mà d'obra directa, però també utilitza mà d'obra indirecta per alguns projecte o per èpoques puntuals.

L'empresa ofereix diferents serveis que s'explicaran a continuació. La principal diferenciació d'aquesta empresa amb d'altres del mateix sector és el alt nivell personalitzat en els serveis. En comptes de vendre molts productes econòmics d'autogestió, opta per oferir productes molt personalitzats, evidentment amb un cost més elevat, però oferint el tracte directe amb el client i la gestió i administració dels seus recursos.

- **Serveis Cloud:**

  S'ofereixen serveis basats en plataformes. Les plataformes van des de CRM, ERP, Servidors dedicats, Servidors Virtuals, Hosting Web, Telefonia IP, etcètera.

  La diferència principal entre aquest servei i el típic servei cloud és que totes les plataformes que s'ofereixen, són gestionades i administrades per l'empresa XX. És tracta d'oferir al client una externalització dels seus sistemes i que aquests siguin gestionats i administrats per la Empresa XX. És un servei pensat per PYMEs que no disposin d'un servei informàtic a l'empresa i vulguin externalitzar el departament al complet.

- **Serveis en Sistemes**

  Es realitza la consultoria, la gestió i l'administració dels sistemes locals o externs del client.

- **Serveis en Xarxes**

S'implanten i es dissenyen les xarxes dels clients a tots els nivells. Des de una xarxa VPN, un Firewall, VLANs, etcètera. Normalment aquest servei està més enfocat a grans companyies que necessiten comunicar seus o empreses que disposen dels seus propis sistemes.

- **Seguretat Informàtica**

És gestiona la seguretat dels clients, principalment a nivell tècnic, tot i que també es desenvolupen plans de seguretat per a establir procediments correctes amb les TIC.

- **Assistència Tècnica**

Es gestionen les incidències a nivell ofimàtic dels clients. El 90% de les incidències es resolen remotament amb el software de control remot TeamViewer. En el 10% de les incidències, un tècnic s'ha de desplaçar per solucionar el problema.

- **Gestió de CPDs**

L'empresa disposa d'un CPD propi on allotja els seus propis sistemes. A part, en aquest CPD, és on ofereix els serveis Cloud als seus clients.

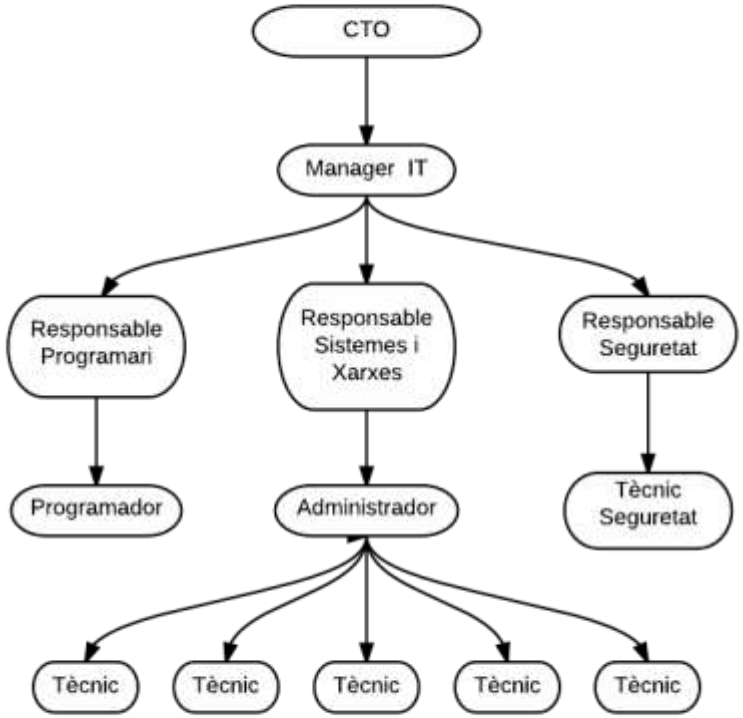
- **Desenvolupament de Plataformes**

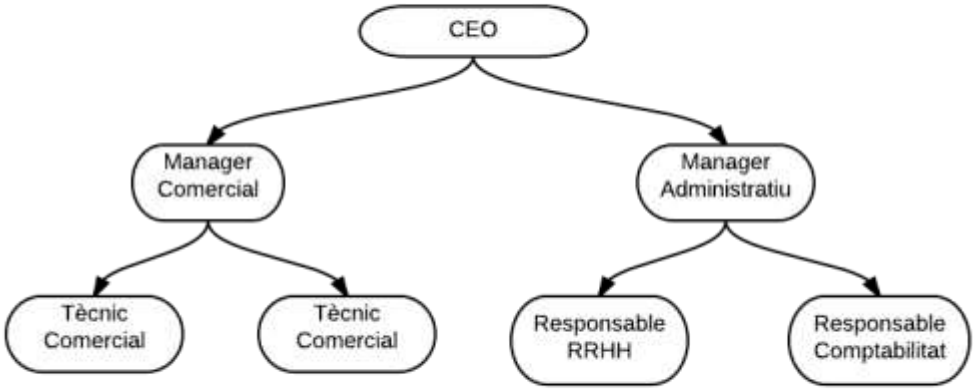
Es desenvolupen, es gestionen i s'administren plataformes a mida o OpenSource per als clients. Normalment es tracten de CRMs, ERPs, Clouds Privats o diferents plataformes adaptades a les necessitats dels clients.

- **Outsourcing**

És un servei molt enfocat a mitjanes i grans empreses i l'objectiu és la cessió temporal de personal format i amb amplis coneixements. Les cessions es realitzen per projectes concrets o funcions especifiques on un tècnic especialitzat els hi gestiona aquest projecte o els ajuda al seu desenvolupament.

Organigrama





Com es pot observar a l'organigrama, l'empresa centra la gran part dels seus recursos en el departament IT, nucli principal del negoci.

La part IT està formada per un CTO (Director Tecnològic) i les seves funcions son les de dirigir i guiar a l'empresa amb una millora continuada del negoci, buscant noves solucions al mercat i mirant quines es poden aplicar i adaptar a l'empresa.

Seguidament hi ha la figura del Manager IT. Aquesta persona es la responsable de gestionar els projectes i serveis relacionats amb IT. També es la persona que barreja coneixements tècnics amb habilitats comercials, per aquest motiu reuneix amb els clients actuals i els possibles futurs clients juntament amb el manager comercial.

D'ell pengen tres rols més, els responsables de Programació, de Seguretat i de Xarxes i Sistemes. El que té un pes més específic en aquests rols és el Responsable de Xarxes i Sistemes, ja que ha de gestionar un grup de persones i projectes on es centra l'activitat principal de l'empresa.

En el següent nivell, es troba l'administrador de la xarxa. És la persona amb més coneixements tècnics i la qual gestiona i administra el CPD i els sistemes dels clients.

Finalment, pel que fa a la secció IT, es troben els tècnics. Hi ha dos tècnics, un de seguretat i l'altre de programació, que es dediquen a realitzar, juntament amb els seus responsables, les tasques corresponents al seu departament. La resta de tècnics pengen del departament de xarxes i sistemes, ja que es l'activitat que més volum requereix. Aquests tècnics s'encarreguen de donar solucions tècniques als clients, de gestionar, juntament amb l'administrador el CPD i els sistemes. Cada un d'ells té un rol més específic per tal de cobrir els diferents serveis que ofereix l'empresa.

Per altra banda, es troba el departament comercial i d'administració.

Hi ha una figura principal que és el CEO (Director General), el qual s'encarrega, juntament amb el CTO, de dirigir i encaminar el model de negoci, però es centra més en aspectes empresarials i econòmics.

D'aquí pengen els responsables d'administració i el responsable comercial. El responsable comercial te al seu càrrec a dos tècnics comercials que l'ajuden a dur a terme les tasques de captació de clients i de compres.

Finalment el departament administratiu té a una persona encarregada dels recursos humans, la qual també combina la seva feina amb tasques de secretaria, i la persona encarregada de comptabilitat, la qual porta l'estat els comptes i la economia de l'empresa, juntament amb el manager administratiu.

Finalment el departament administratiu té a una persona encarregada dels recursos humans, la qual també combina la seva feina amb tasques de secretaria, i la persona encarregada de comptabilitat, la qual porta l'estat els comptes i la economia de l'empresa, juntament amb el manager administratiu.

Instal·lacions

L'empresa XX té la seva seu a Mataró, on disposa d'oficines d'uns 200 m^2 a la 2a planta d'un parc tecnològic.

L'empresa també disposa d'un CPD propi de 20 m^2 on té ubicats els seus sistemes i els dels clients. Aquest CPD està ubicat a la planta -1 de l'edifici, per tant, està separat de les oficines.

La oficina està a la segona planta d'un dels edificis, el qual ubica a quatre empreses per planta. Cada empresa té una cantonada de l'edifici i les quatre empreses comparteixen els lavabos.

Per accedir a les oficines, els empleats ho fan amb targetes magnètiques personals, les quals han de passar per un lector per tal que s'activi l'obertura de la porta a les oficines. En principi aquestes targes només tenen accés a la porta de l'oficina, tot i que hi ha diferents perfils. El perfil treballador, només té accés a les oficines durant el horari laboral, un cop tancat l'edifici no hi té accés. El perfil empresari té accés tant a la part exterior de l'edifici, per quan aquest està tancat poder-hi accedir, com a les oficines i al parking.

L'edifici està controlat amb càmeres de seguretat en cada pis i amb varies al Hall. Aquestes càmeres son supervisades per l'equip de seguretat de l'edifici 24h al dia. A més, l'edifici disposa d'un conserge, al Hall, per la recepció de visites i correspondència.

L'edifici consta de diverses alarmes, les quals es desactiven amb les targetes magnètiques d'entrada a les oficines. Aquestes alarmes, només estan activades en el horari en que està tancat l'edifici.

També hi ha un servei de neteja que te accés a les oficines en el horari de 20.00 a 22.00h.

A part dels sistemes de seguretat d'alarmes i videocàmeres, l'empresa no disposa de cap propi per dins de les oficines.

Si que te dues videocàmeres instal·lades al CPD, però que no son monitoritzades constantment per ningú. De totes maneres realitzen còpies les 24h.

Per accedir al CPD també s'ha d'utilitzar la targeta magnètica. Per tal de sortir del CPD també s'ha d'utilitzar la targeta magnètica. D'aquesta manera queda un registre de qui ha entrat i quan ha sortit del CPD. Només tenen accés alguns tècnics, l'administrador, els responsables i els directors.

Les oficines disposen de 5 llocs tancats. Els dos despatxos dels directors, una sala gran on s'ubiquen el departament comercial i el d'administració, i una sala de reunions. La resta de les oficines, tret d'una última sala, es un espai obert on hi ha una recepció, lloc que ocupa la persona de RRHH, ja que comparteix tasques de RRHH i de secretaria, una illeta de quatre llocs de treball pel manager i els tres responsables de la secció IT, i unes altres dues illetes de quatre on s'ubiquen els tècnics, el programador i el administrador. A la zona dels tècnics i l'administrador, la més propera a la paret, hi ha 4 monitors de 50 polsades amb la monitorització del CPD i dels clients.

Finalment hi ha una última sala, bastant petita, que es on es guarden els arxius en paper, documents, cintes de gravació, còpies de seguretat, etcètera, els quals estan tancats en armaris sota clau.

Dins de l'edifici hi ha una zona destinada al menjador, on els treballadors poden menjar i on hi ha màquines dispensadores i de cafè.

CPD - Sistemes Propis

Pel que fa al nivell de sistemes de l'empresa, aquests estan ubicats al mateix CPD que els clients.

Aquest CPD està refrigerat i consta de quatre RACKs de 40U. Un dels RACKs està vuit i pensat per un futur creixement. Dels altres tres, cada RACK disposa de dos SAIs de 3600W on es pengen els diferents equips.

El primer RACK està destinat al conexionat. Consta de:

- Un patch pannel que prové de l'oficina.
- 4 switches gestionables, de la marca enterasys, que separen les xarxes per vlans.
- 2 routers amb dues línies de fibra proporcionades per proveïdors diferents amb la finalitat de garantir una major disponibilitat. Hi ha contractat 200 Mb simètrics per cada fibra. Un operador es COLT i l'altre Orange.
- 2 routers ADSL que s'utilitzen per les línies telefòniques, per la sortida d'emergència en cas que fallin les dues fibres i per donar accés a internet a les visites.

- 2 firewalls, els quals a part de filtrar continguts, de monitoritzar les connexions i de donar seguretat, també permeten l'accés VPN.
- 1 balancejador de càrrega per tal de garantir l'accés a Internet i de balancejar entre les dues línies de fibra que hi ha per tal d'evitar saturació.

Tots els equips d'aquest RACK, tret del balancejador, estan replicats i per tant donen redundància al servei.

La meitat del segon RACK s'utilitza per ubicar els sistemes de l'empresa XX.
L'empresa treballa amb tecnologia de virtualització, concretament amb VMWare. Dins de cada servidor físic s'allotgen diferents màquines. En la primera meitat del segon RACK hi ha 4 servidors HP, dues cabines de discos ISCSI, també de la marca HP, i un robot de cintes.

L'empresa XX disposa dels següents sistemes:

Servidor 1:

- VM - Domain Controller

  Aquest equip te instal·lat el SO Windows Server 2008, i te configurat un Active Directory, el servei DNS i el DHCP.
- VM – Servidor de fitxers

  Windows Server 2008 amb una alta capacitat de disc on s'ubiquen tots els documents de l'empresa i els quals estan filtrats per permisos d'accés.
- VM – Servidor de correu

  Aquest equip te instal·lat el SO Windows Server 2008, amb la Exchange 2010 i és l'equip que s'encarrega del correu corporatiu de l'empresa XX.

- VM – Base de dades Microsoft

  Servidor amb un WS 2008 instal·lat i amb el SQL també instal·lat. Aquí es on s'ubiquen les dades del ERP i del vCenter.

Servidor 2:

- VM – Servidor WEB

  Pel servidor Web es fa servir un Linux, concretament CentOS 6, on s'ubica la pàgina web de l'empresa.

- VM – ERP

  Màquina amb WS 2008 i l'aplicatiu ERP instal·lat.
- VM – CRM

  Màquina amb Linux i el CRM que utilitza el departament comercial configurat.
- VM – Monitorització Intern

  Màquina amb Centos 6 i el sistema nagios configurat. S'utilitza per la monitorització dels sistemes locals, tant servidors com switches, router, etc.
- VM – Monitorització Extern

  Màquina amb Centos 6 i el sistema nagios configurat. S'utilitza per la monitorització dels equips dels clients.

Servidor 3:

- VM – Backup Local

  SO Windows Server 2008, amb l'aplicació Veeam Backup, la qual gestiona tot el tema de còpies de màquines virtuals a una de les cabines.
- VM – Backup Cintes

  SO Windows Server 2008, amb l'aplicació ArcServe, la qual gestiona tot el tema de còpies en cintes.
- VM – vCenter

  Es una màquina amb WS 2008 i amb el vCenter de VMWare instal·lat. Aquest aplicatiu el que permet és moure màquines entre hosts en calent per tal d'optimitzar recursos o com a mesura de precaució. A més, et dona una visió i una gestió global de l'entorn de virtualització.
- VM – Centraleta + Base de dades Linux

  Servidor amb CentOS instal·lat i utilitzat com a base de dades de la pàgina web i el CRM, els quals son Open Source. Pel que fa la web s'utilitza Wordpress i pel CRM s'utilitza vTiger. A part també té instal·lat l'aplicatiu Asterisk que gestiona la centraleta.
- VM – Gravacions càmeres.

  Un sistema CentOS amb un software que emmagatzema les gravacions de les càmeres del CPD.

Servidor 4:

Aquest servidor està destinat totalment a proves o com a servidor de Backup per si un dels altres fallés.

CPD – Sistemes Externs

La meitat del segon RACK i el tercer està destinat a ubicar les màquines dels clients.

Els equips que s'utilitzen son els mateixos que els propis, servidors i cabines de discos HP.

Hi ha clients que contracten VM i hi ha d'altres que contracten servidors dedicats.

En total hi ha 20 servidors destinats als clients. Entre els totes les màquines, virtuals i físiques hi ha un 60% de Linux i un 40% Windows.

Oficines – Sistemes Propis

Pel que fa als sistemes dels empleats, tots el equips que utilitzen els empleats son portàtils. D'aquesta manera s'unifica la metodologia dels equips i es permet el teletreball ja que cada usuari el pot portar el equip a casa. Per poder realitzar la connexió ho fan a través de la VPN.
L'empresa utilitza la marca Lenovo.

Els portàtils es poden diferenciar en tres gammes:

- Portàtil Direcció

  Son ultrabooks amb un processador i5 disc SSD, 6 GB RAM i els utilitzen els directors i els managers.

- Portàtil Tècnic

  Son portàtils robustos de 14'', i5 amb 8GB RAM. El fan servir tots els tècnics de la secció IT i l'administrador

- Portàtil Bàsic

  Es un portàtil bàsic de 14'', i3 amb 4 GB RAM i el fan servir els tècnics comercials i el personal d'administració.

Equipament Usuaris:

- Tots els equips tenen instal·lats de base el sistema operatiu Windows 7 versió Profesional i amb Office 2010.
- Tots els equips estan units al domini de l'empresa.
- Tenen una assignació d'IP per MAC
- El directors compten amb Iphone 5s i IPAD
- Els managers també disposen de tablets IPAD i Iphone 5

- Els tècnics comercials porten tabletes android i mòbils android.
- A cada lloc de treball hi ha com a mínim un monitor de 21'' amb el peu regulable i teclat + ratolí + dock station. Hi ha alguns treballadors, sobretot a la part tècnica que utilitzen varis monitors.

Xarxa:

- Tots els equips funcionen amb ethernet.
- La ethernet funicona a 1 Gbps
- Hi ha un Acces Point per poder connectar els dispositius mòbils i tablets i per utilitzar la xarxa a la sala de reunions.
- Pel que fa a la Wifi, hi ha dos SSID, el corporatiu que funciona amb autenticació 802.1x i el públic per les visites que està protegit amb password i totalment aïllat de la xarxa.

Altres aspectes:

- Hi ha 3 PCs en format barebone connectats a les 3 pantalles de 50'' per tal de veure la monitorització que realitza el nagios.
-

2.1.2 Abast

L'abast del pla director de l'empresa XX és vol garantir la seguretat de la informació de la pròpia empresa en la seva totalitat, des de procediments i polítiques fins els aspectes tècnics per mitigar les diferents amenaces que es puguin provocat. També es fonamental garantir la seguretat dels clients que tenen els seus sistemes ubicats al CPD de l'empresa XX. Es volen garantir uns SLA amb els clients, per tant el pla director ha d'abastir la redundància en els serveis que s'ofereixen.

2.2 Objectius

Amb el pla director, l'empresa pretén obtenir un nivell de seguretat de la informació superior a l'actual. L'empresa vol garantir diversos aspectes:

- Es vol garantir la disponibilitat de recursos dels clients que tenen els seus sistemes al CPD de l'empresa XX.
- Es vol garantir que les dades que tenen els clients ubicades al CPD tenen un risc molt petit de pèrdua.
- Es vol garantir la protecció de dades privades dels clients.
- Es vol garantir que les dades dels clients estan totalment protegides enfront a fugues d'informació, tant per part d'atacants com de personal intern.
- Es vol demostrar que l'empresa té uns controls i uns procediments de seguretat òptims amb la finalitat de donar un valor afegit al servei que ofereixen.
- Es vol evitar que el knowhow de l'empresa pugui arribar a la competència degut a una fuga d'informació interna.
- Es vol evitar que el codi les aplicacions pròpies pugui ser robat o extret de l'empresa.
- Es vol establir un procés de millora continuada enfront a la seguretat, amb revisions periòdiques del compliment dels controls i els procediments aplicats.

2.3 Anàlisis diferencial

Per tal de veure la situació actual de l'empresa, s'ha realitzat un anàlisi diferencial enfront a la norma ISO 27002:2013.

5. POLÍTICAS DE SEGURIDAD

Objetivo	Control	SI	NO
5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información.		X
	5.1.2 Revisión de las políticas para la seguridad de la información.		X

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo	Control	SI	NO
6.1 Organización interna	6.1.1 Asignación de responsabilidades para la segur. de la información.	X	
	6.1.2 Segregación de tareas.		X
	6.1.3 Contacto con las autoridades.		X
	6.1.4 Contacto con grupos de interés especial.		X
	6.1.5 Seguridad de la información en la gestión de proyectos.		X
6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad.		X
	6.2.2 Teletrabajo.	X	

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Objetivo	Control	SI	NO
7.1 Antes de la contratación	7.1.1 Investigación de antecedentes.		X
	7.1.2 Términos y condiciones de contratación.	X	
7.2 Durante la contratación	7.2.1 Responsabilidades de gestión.		X
	7.2.2 Concienciación, educación y capacitación en segur. de la informac.		X
	7.2.3 Proceso disciplinario.		X
7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo.		X

8. GESTIÓN DE ACTIVOS

Objetivo	Control	SI	NO
8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos		X
	8.1.2 Propiedad de los activos		X
	8.1.3 Uso aceptable de los activos.		X
	8.1.4 Devolución de activos		X
8.2 Clasificación de la información	8.2.1 Directrices de clasificación.	X	
	8.2.2 Etiquetado y manipulado de la información	X	
	8.2.3 Manipulación de activos		X
8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles		X
	8.3.2 Eliminación de soportes.		X
	8.3.3 Soportes físicos en tránsito		X

9. CONTROL DE ACCESOS

Objetivo	Control	SI	NO
9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos.		X
	9.1.2 Control de acceso a las redes y servicios asociados.	X	
9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios.	X	
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	X	
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	X	
	9.2.4 Gestión de información confidencial de autenticación de usuarios.		X
	9.2.5 Revisión de los derechos de acceso de los usuarios.		X
	9.2.6 Retirada o adaptación de los derechos de acceso		X
9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación		X
9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información.	X	
	9.4.2 Procedimientos seguros de inicio de sesión.	X	
	9.4.3 Gestión de contraseñas de usuario.	X	
	9.4.4 Uso de herramientas de administración de sistemas		X
	9.4.5 Control de acceso al código fuente de los programas.		X

10. CIFRADO

Objetivo	Control	SI	NO
10.1 Controles criptográficos.	10.1.1 Política de uso de los controles criptográficos		X
	10.1.2 Gestión de claves		X

11. SEGURIDAD FÍSICA Y AMBIENTAL

Objetivo	Control	SI	NO
11.1 Áreas seguras	11.1.1 Perímetro de seguridad física.	X	
	11.1.2 Controles físicos de entrada		X
	11.1.3 Seguridad de oficinas, despachos y recursos.		X
	11.1.4 Protección contra las amenazas externas y ambientales.		X
	11.1.5 El trabajo en áreas seguras.		X
	11.1.6 Áreas de acceso público, carga y descarga.		X
11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos.		X
	11.2.2 Instalaciones de suministro		X
	11.2.3 Seguridad del cableado.		X
	11.2.4 Mantenimiento de los equipos.	X	
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	X	
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.		X
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.		X
	11.2.8 Equipo informático de usuario desatendido.		X
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.		X

12. SEGURIDAD EN LA OPERATIVA

Objetivo	Control	SI	NO
12.1 Responsabilidades y procedimientos de operación.	12.1.1 Documentación de procedimientos de operación.		X
	12.1.2 Gestión de cambios.		X
	12.1.3 Gestión de capacidades.	X	
	12.1.4 Separación de entornos de desarrollo, prueba y producción.		X
12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.	X	
12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.	X	
12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad.		X
	12.4.2 Protección de los registros de información.		X
	12.4.3 Registros de actividad del administrador y operador del sistema.		X
	12.4.4 Sincronización de relojes.		X
12.5 Control del software en explotación.	12.5.1 Instalación del software en sistemas en producción.		X
12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.		X
	12.6.2 Restricciones en la instalación de software.		X
12.7 Consideraciones de las auditorías de los sistemas de información.	12.7.1 Controles de auditoría de los sistemas de información.		X

13. SEGURIDAD EN LAS TELECOMUNICACIONES

Objetivo	Control	SI	NO
13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.	X	
	13.1.2 Mecanismos de seguridad asociados a servicios en red.		X
	13.1.3 Segregación de redes.	X	
13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información.		X
	13.2.2 Acuerdos de intercambio.		X
	13.2.3 Mensajería electrónica.	X	
	13.2.4 Acuerdos de confidencialidad y secreto.		X

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo	Control	SI	NO
14.1 Requisitos de seguridad de los sistemas de información.	14.1.1 Análisis y especificación de los requisitos de seguridad.		X
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas		X
	14.1.3 Protección de las transacciones por redes telemáticas.		X
14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.1 Política de desarrollo seguro de software.		X
	14.2.2 Procedimientos de control de cambios en los sistemas.		X
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	X	
	14.2.4 Restricciones a los cambios en los paquetes de software.	X	
	14.2.5 Uso de principios de ingeniería en protección de sistemas.		X
	14.2.6 Seguridad en entornos de desarrollo.	X	
	14.2.7 Externalización del desarrollo de software.	X	
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	X	
	14.2.9 Pruebas de aceptación.		X
14.3 Datos de prueba.	14.3.1 Protección de los datos utilizados en pruebas.		X

15. RELACIONES CON SUMINISTRADORES

Objetivo	Control	SI	NO
15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores.		X
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.		X
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.		X
15.2 Gestión de la prestación del servicio	15.2.1 Supervisión y revisión de los servicios prestados por terceros.		X

por suministradores.	15.2.2 Gestión de cambios en los servicios prestados por terceros.		X

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo	Control	SI	NO
16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos.	X	
	16.1.2 Notificación de los eventos de seguridad de la información.		X
	16.1.3 Notificación de puntos débiles de la seguridad.		X
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.		X
	16.1.5 Respuesta a los incidentes de seguridad.		X
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.		X
	16.1.7 Recopilación de evidencias.		X

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo	Control	SI	NO
17.1 Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información.		X
	17.1.2 Implantación de la continuidad de la seguridad de la información.		X
	17.1.3 Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.		X
17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	X	

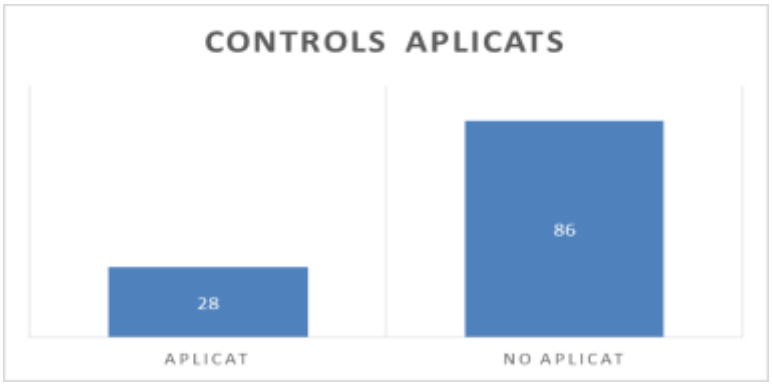
18. CUMPLIMIENTO

Objetivo	Control	SI	NO
18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.		X
	18.1.2 Derechos de propiedad intelectual (DPI).		X
	18.1.3 Protección de los registros de la organización.		X
	18.1.4 Protección de datos y privacidad de la información personal.		X
	18.1.5 Regulación de los controles criptográficos.		X
18.2 Revisiones de la seguridad de la	18.2.1 Revisión independiente de la seguridad de la información.		X

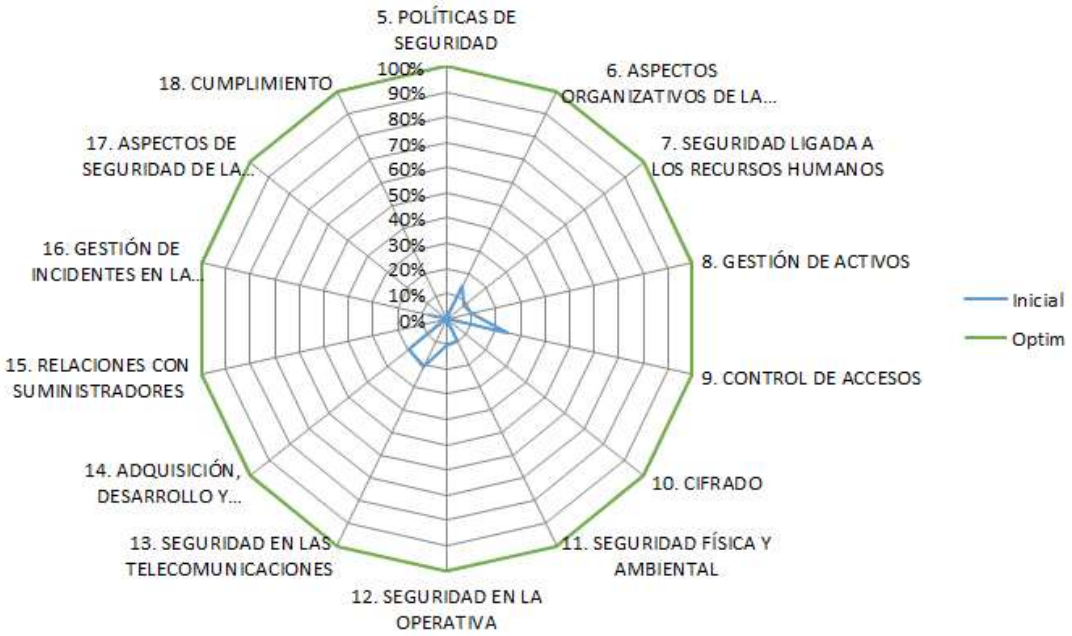
información.	18.2.2 Cumplimiento de las políticas y normas de seguridad.		X
	18.2.3 Comprobación del cumplimiento.		X

2.4 Resum Executiu

Com es pot observar en el següent gràfic, l'empresa té un alt percentatge de controls NO APLICATS. Donada la seva activitat es indispensable crear un pla director per tal d'aplicar tots els controls que demana la ISO 27002. La gran majoria dels controls no aplicats venen donats per la part de procediments i polítiques de seguretat. En l'aspecte tècnic ja s'estan aplicant alguns d'ells, tot i que n'hi ha d'altres fonamentals per la seguretat del negoci que no s'estan aplicant encara.



En el següent gràfic podem veure el nivel de controls aplicats a l'empresa enfront al nivell optim d'aplicació.



3. Sistema de Gestió Documental

3.1 Política de Seguretat

La política de seguretat de la informació persegueix els següents objectius:

- Definir una sèrie de protocols que assegurin una protecció a la informació de l'empresa.
- Establir uns procediments que garanteixin el ús correcte dels recursos de la informació dins de l'empresa.
- Definir els aspectes relatius als accessos a la informació.
- Definir el comportament del personal enfront a situacions crítiques o d'emergència.

3.2 Procediment d'Auditories Internes

L'objectiu d'aquest procediment és planificar les auditories que es durant a terme durant la vigència del certificat obtingut un cop finalitzat el SGSI.

El document defineix:

- Amb quina periodicitat es realitzaran les auditories
- Tipus de auditories que es realitzaran, de control o tècniques.
- Nivell de les auditories que es realitzaran.

3.3 Gestió d'indicadors

L'objectiu d'aquest document és definir els indicadors necessaris per tal de mesurar amb la màxima eficiència dels controls establerts al pla director.

3.4 Procediment de Revisió per Direcció

L'objectiu d'aquest document és definir el procediment a realitzar per la gerència de l'empresa amb la finalitat de la revisió i supervisió del correcte funcionament del SGSI.

3.5 Gestió de Rols i Responsabilitats

L'objectiu d'aquest document és definir l'equip que s'encarregarà de crear mantenir, supervisar i millorar el Sistema de gestió de la informació. Aquest equip serà definit com el comitè de seguretat.

3.6 Metodologia d'Anàlisi de Riscos

L'objectiu d'aquest document és definir la metodologia que s'utilitzarà per tal de calcular el risc en els procediments de l'empresa.

3.7 Declaració d'Aplicabilitat

L'objectiu d'aquest document és definir tots els controls de Seguretat establerts a la Empresa XX amb el detall de la seva aplicabilitat, el seu estat i la documentació relacionada.

4. Anàlisis de riscos

4.1 Inventari d'Actius

En aquest punt s'avaluaran els actius de l'empresa, considerant les dependències entre ells i fent la valoració del mateixos.

Per tal d'inventariar els actius de l'empresa, es classificaran en diferents grups, tot seguint la metodologia MAGERIT. Els grups d'actius són:

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

Donat que hi ha certs actius dels quals l'empresa es beneficia però que no formen part de l'empresa, ja que els proporciona el parc on està ubicada, no es contemplen directament com actius. Un exemple podria ser el conserge, l'equip de seguretat, el sistema d'alarmes, les càmeres o el menjador.

4.2 Valoració dels actius

En aquest apartat es determinarà el valor dels actius dins de l'organització. Per realitzar aquesta valoració ens basarem en l'anàlisi que proposa MAGERIT completant-lo amb una valoració quantitativa.

Valoració dels Actius		
Tipus	**Abreviatura**	**Valor**
Molt Baix	MB	1.000€
Baix	B	5.000€
Mig	M	10.000€
Alt	A	50.000€
Molt Alt	MA	100.000€

4.3 Dimensions de seguretat

En aquest apartat es mesura la criticitat a les cinc dimensions de la seguretat de la informació dins de l'organització. Aquesta valoració permetrà valorar l'impacte que tindrà una certa amenaça sobre un actiu en concret.

Les cinc dimensions de la seguretat de la informació són les següents:

- **Autenticitat:** es la propietat que prova qui és l'autor de la informació.
- **Confidencialitat:** és la propietat que impedeix la divulgació de la informació a persones o sistemes no autoritzats.
- **Integritat:** és la propietat que busca mantenir les dades lliures de modificacions no autoritzades.
- **Disponibilitat:** és la característica de la informació de trobar-se sempre a disposició de qui ha d'accedir a ella.
- **Traçabilitat:** és la propietat que permet determinar totes i cada una de les accions que realitza cada usuari.

A les diferents dimensions de la seguretat se'ls hi ha d'assignar un valor en funció de la rellevància que tinguin per un actiu en concret. Per determinar aquest valor es farà servir la següent taula:

Valor	Criteri
10	Dany molt greu
7-9	Dany greu
4-6	Dany important
1-3	Dany menor
0	Dany irrellevant

4.4 Anàlisi d'amenaces

En aquest apartat es tractaran les amenaces que poden afectat als sistemes d'informació de l'empresa.

Per tal de classificar les amenaces s'han utilitzat les que hi figuren en MAGERIT al seu 2n llibre.

Segons MAGERIT, les amenaces es poden classificar en quatre blocs:

- Desastres naturals.
- D'origen industrial.
- Error i fallides no intencionades.
- Atacs malintencionats.

En el document SardanesLobatoEsteban_A03_02_Analisi_Risc.xls es classifiquen les diferents amenaces.

Freqüència			
Descripció	**Abreviatura**	**Valor**	**Freqüència**
Extremadament freqüent	EF	0,9973	Menys que 1 dia
Molt freqüent	MF	0,1425	Menys que 1 setmana
Freqüent	F	0,0329	Menys que 1 mes
Poc freqüent	PF	0,0055	Menys que 6 mesos
Molt poc freqüent	MPF	0,0027	Menys que 1 any
Menyspreable	D	0,0003	Menys que 10 anys

Impacte		
Descripció	**Abreviatura**	**Valor**
Crític	C	90%
Alt	A	75%
Mitjà	M	50%
Baix	B	20%

4.5 Resultats

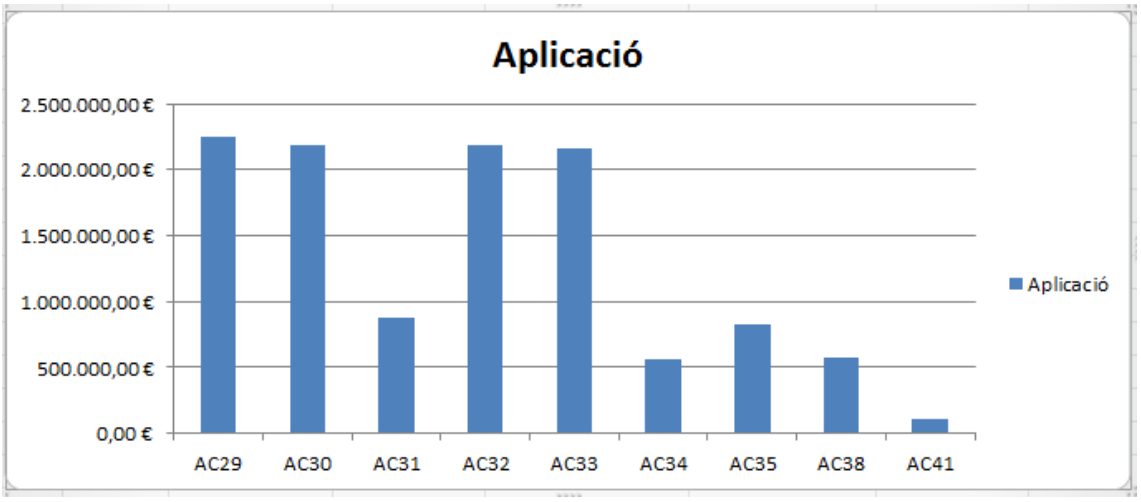
Un cop finalitzar el càlcul de l'impacte potencial de les amenaces en front als actius, en aquest apartat es farà una valoració de quins són els actius més crítics i quines son les amenaces més perilloses.

4.5.1 Actius

Començarem pels actius i farem una valoració dels actius amb més risc classificats per àmbits.

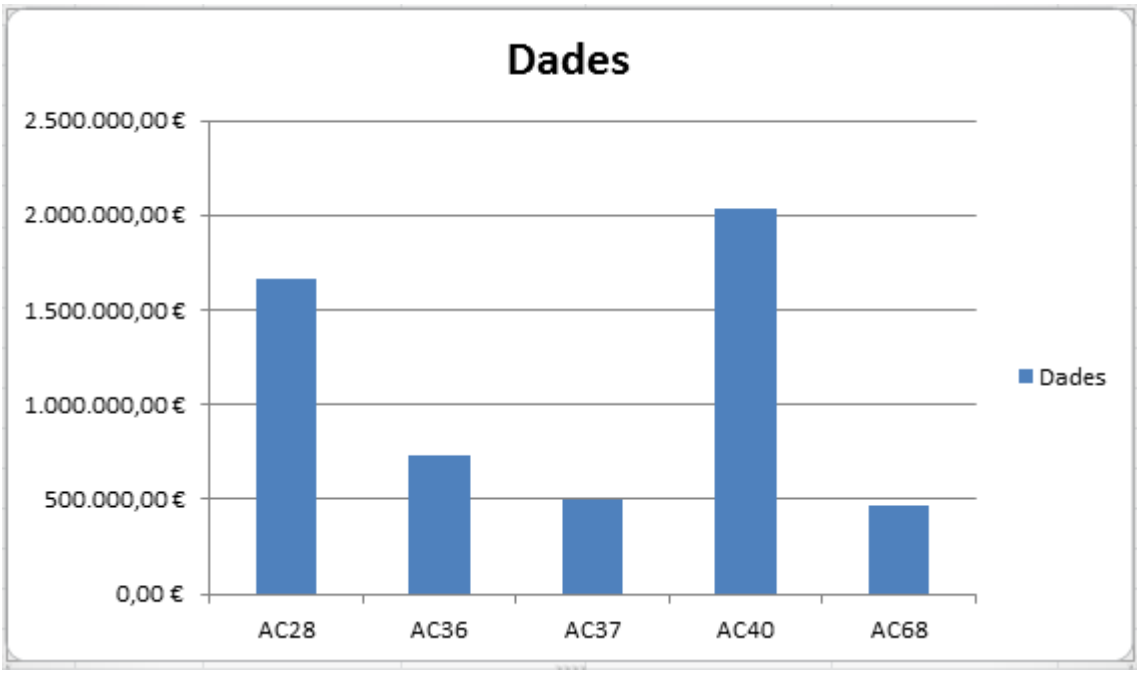
Pel que fa a l'àmbit de les aplicacions, els actius amb més risc són:

- Servidor de Correu
- Servidor de BBDD
- ERP
- CRM



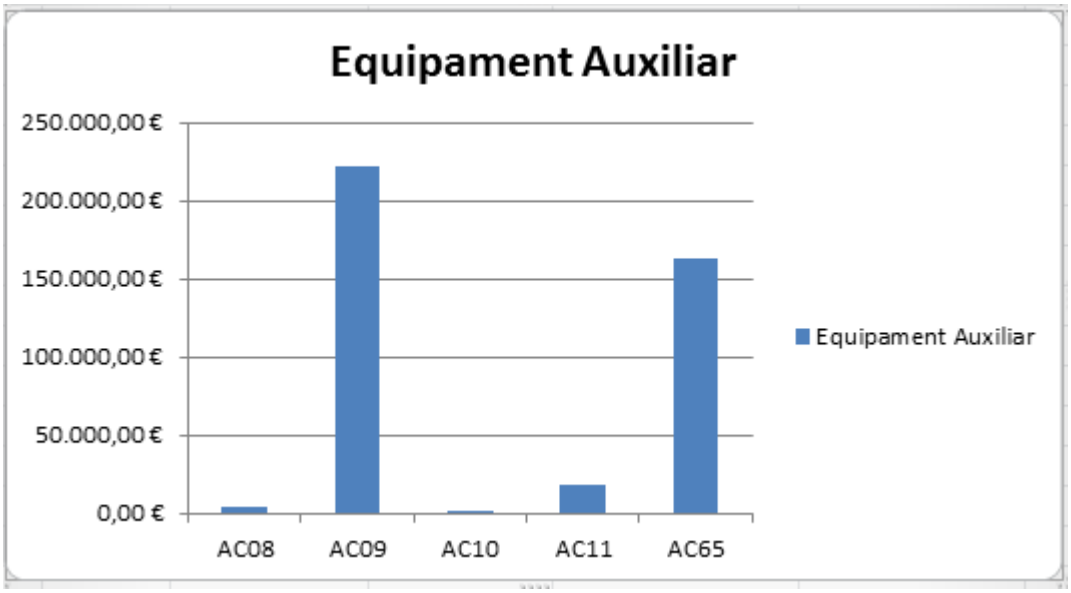
Pel que fa a l'àmbit de les dades els dos actius amb més risc són:

- Repositori de dades
- Base de dades



Pel que fa a l'equipament auxiliar, els dos actius amb més risc són:

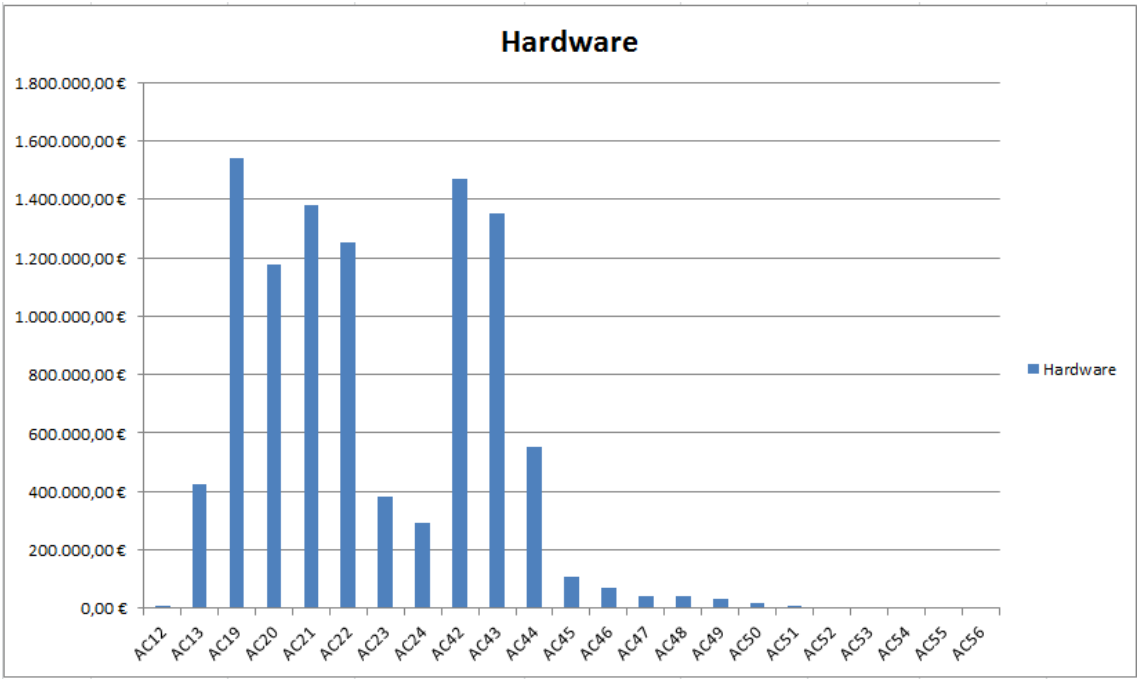
- Càmeres de seguretat
- Subministraments



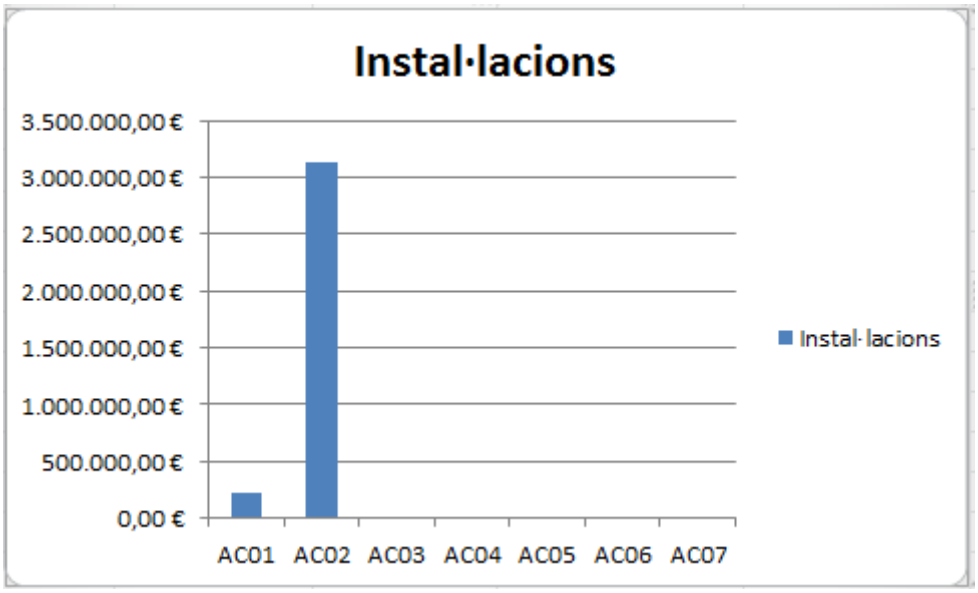
Pel que fa al Hardware, el més crític és el hardware que fa funcionar el negoci:

- Firewalls
- Servidor de l'organització
- Cabines de l'organització
- Servidors dels clients
- Cabines de discos dels clients

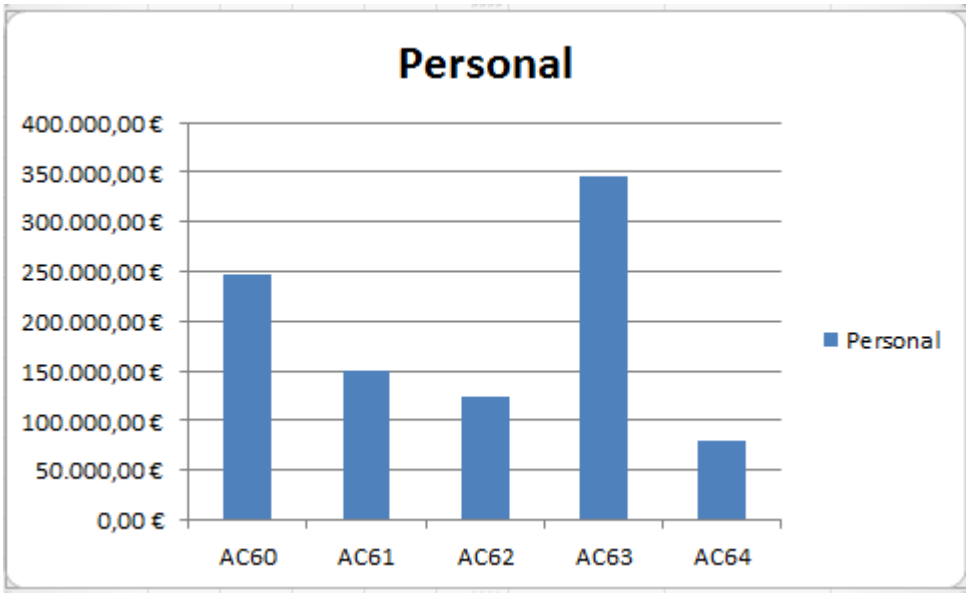
Tot i semblar ser més importants els servidors dels clients, surt amb un risc més alt el Firewall. Això ve donat perquè és el Firewall que dona accés als clients i el que gestiona la comunicació i la seguretat de la comunicació.



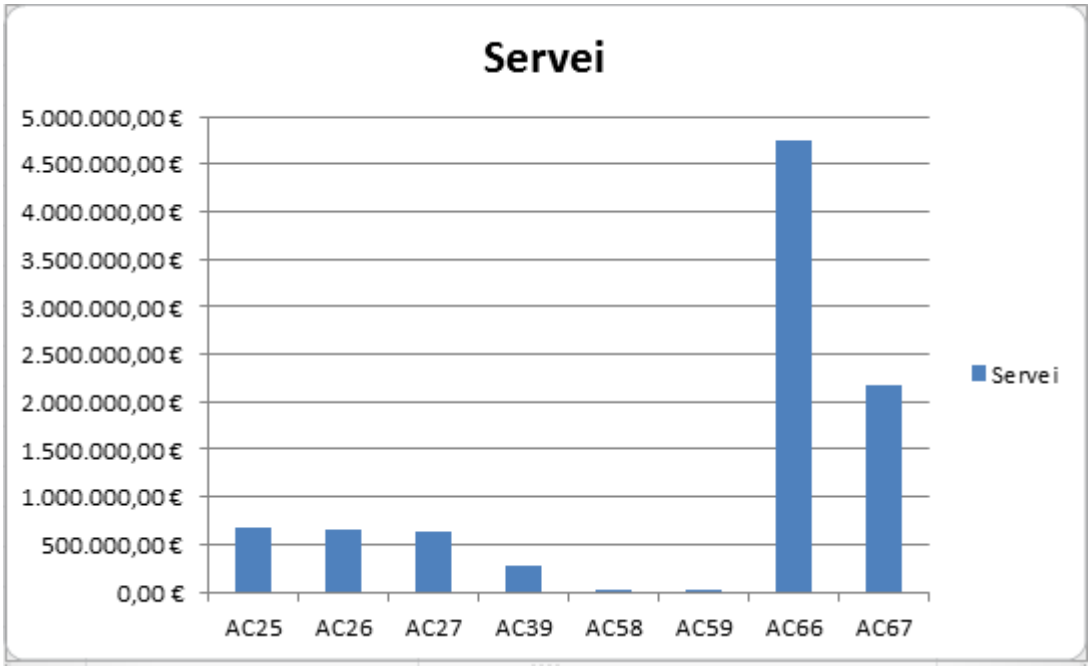
Pel que fa a les instal·lacions, surt molt destacat el CPD, de fer és pràcticament el únic que surt al gràfic donada la gran importància que te el CPD per la organització.



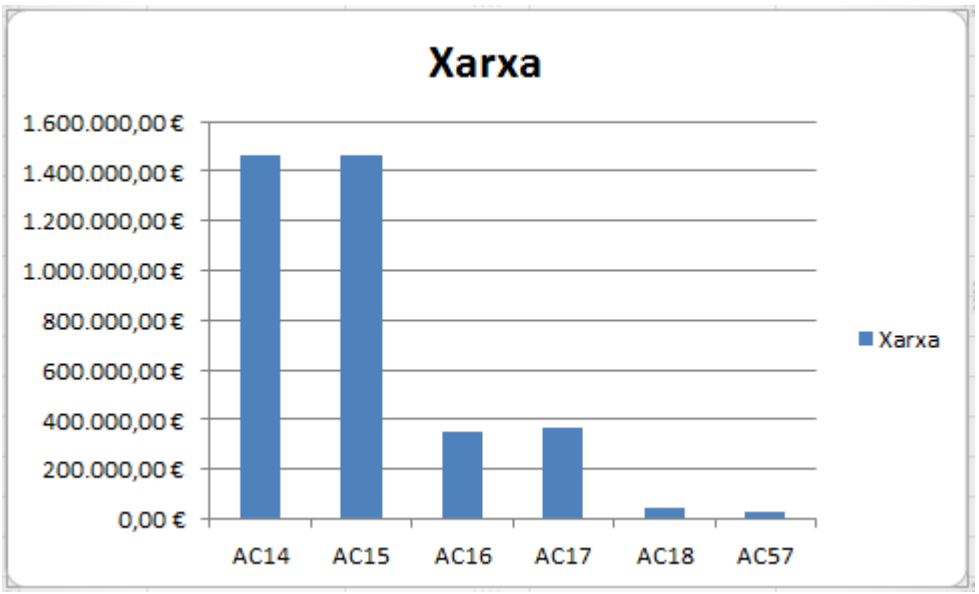
El personal està força igualat a nivell de risc, sent l'administrador l'actiu més destacat. El motiu es perquè és l'administrador que gestiona el CPD, i aquest és l'actiu més important de l'empresa.



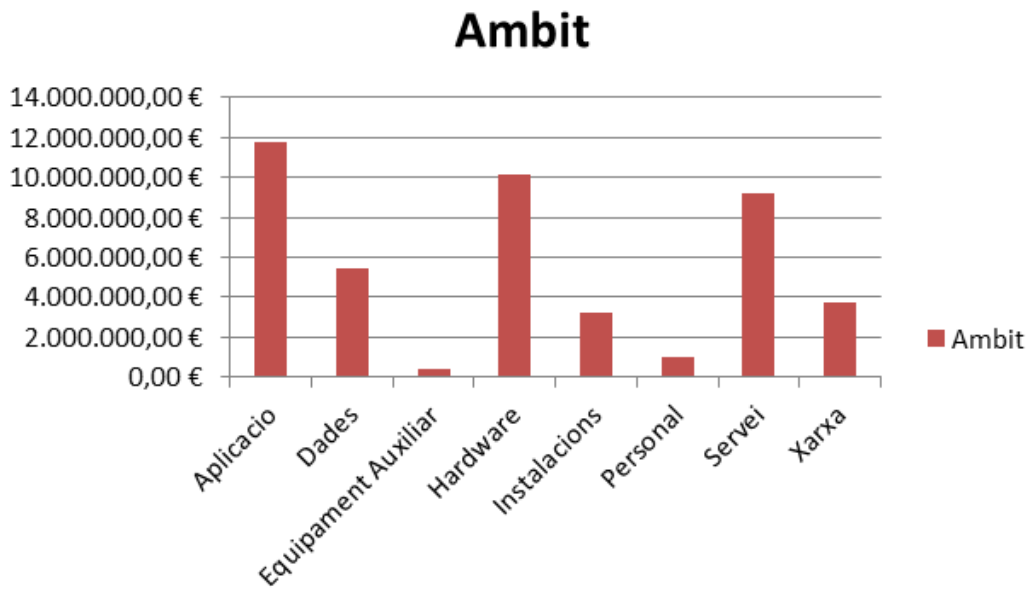
Pel que fa als serveis de l'empresa, el més destacat amb diferencia és el servei que s'ofereix als clients, actiu que genera la gran part dels ingressos de l'organització. Un altre actiu molt important en el servei és el correu electrònic, ja que es la via principal de comunicació dels treballadors i clients.



En l'àmbit de xarxa els actius més importants són els dos routers de fibra que donen funcionament als serveis dels clients, a l'accés a Internet del personal i al funcionament extern del correu electrònic.



Seguidament es mostra una taula amb risc dels diferents àmbits:



Els tres àmbits amb més criticitat son el d'aplicació, el de hardware i el de servei. Aquests són els actius principals que sustenten la disponibilitat dels serveis i per tant la continuïtat del negoci. A nivell d'aplicació trobem actius com el correu electrònic, les BBDD, el ERP o el CRM, eines principals perquè el personal de l'empresa pugui treballar.

El Hardware és un altre dels àmbits amb més risc de l'empresa. És normal ja que per donar servei als clients en disposa de molt.

Seguidament, com a un altre risc crític es troba l'àmbit del servei. És lògic ja que és l'activitat principal del negoci, oferir servei i que aquest estigui disponible.

Finalment, es fa un resum dels actius amb més risc de l'empresa.

AC66	Servei	Serveis TIC dels clients	MA	100.000,00 €	4	8	8	10	2	6,4	13.037,50 €	4.750.687,50 €
AC02	Instal·lacions	CPD	MA	100.000,00 €	4	10	10	10	4	7,6	8.000,00 €	2.952.120,00 €
AC29	Aplicació	Servidor Correu	MA	100.000,00 €	10	10	10	10	10	10	4.154,00 €	2.246.238,00 €
AC30	Aplicació	Sevidor BBDD	MA	100.000,00 €	10	10	10	10	10	10	5.999,50 €	2.189.817,50 €
AC32	Aplicació	ERP	MA	100.000,00 €	10	10	6	8	6	8	5.977,00 €	2.181.605,00 €
AC33	Aplicació	CRM	MA	100.000,00 €	10	10	6	8	6	8	5.932,00 €	2.165.180,00 €
AC67	Servei	Correu Electrònic	MA	100.000,00 €	8	8	8	10	6	8	5.930,50 €	2.164.632,50 €
AC40	Dades	Base de dades	MA	100.000,00 €	10	10	9	10	9	9,6	5.570,50 €	2.033.232,50 €

El actiu que més risc comporta a l'empresa d'una manera destacada és el Servei TIC dels clients. És el actiu principal amb el qual fa negoci l'empresa.

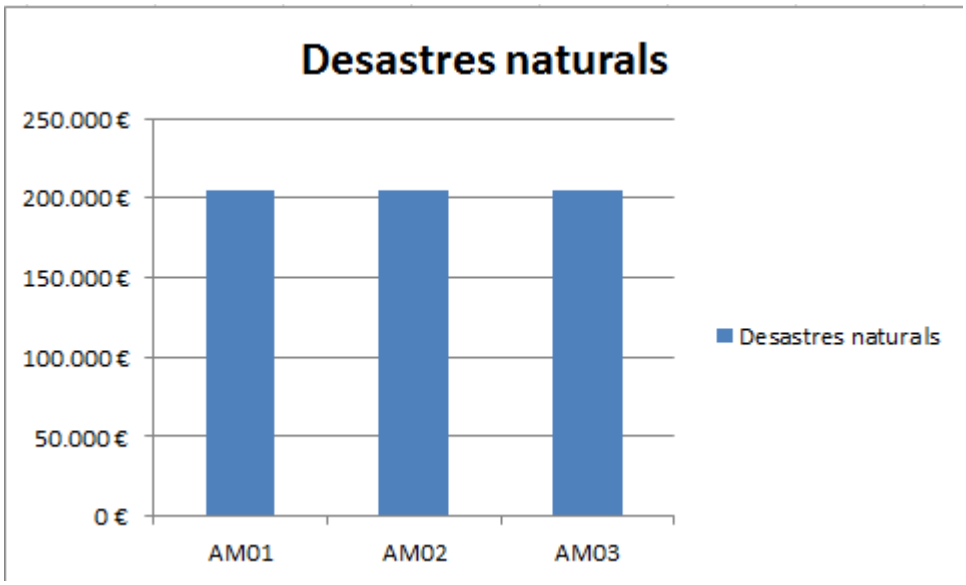
El següent actiu amb més risc de l'empresa és el CPD. Evidentment, els serveis TIC dels clients depenen en una gran part del CPD, d'aquí la gran importància d'aquest.

Els següents actius més importants de l'empresa son el servidor de correu i el servidor de BBDD, ja que son la eina principal de treball i comunicació dels usuaris. D'aquest dos actius també depenen els següents, que fan referencia al servei de correu electrònic i a les dades de la BBDD.

Finalment, veiem que el ERP i CRM son dos altres actius molt elevats, ja que aquí és on figura tot el sistema de facturació i tot el sistema comercial de l'empresa. Aquests dos actius també depenen en gran part del servidor de BBDD.

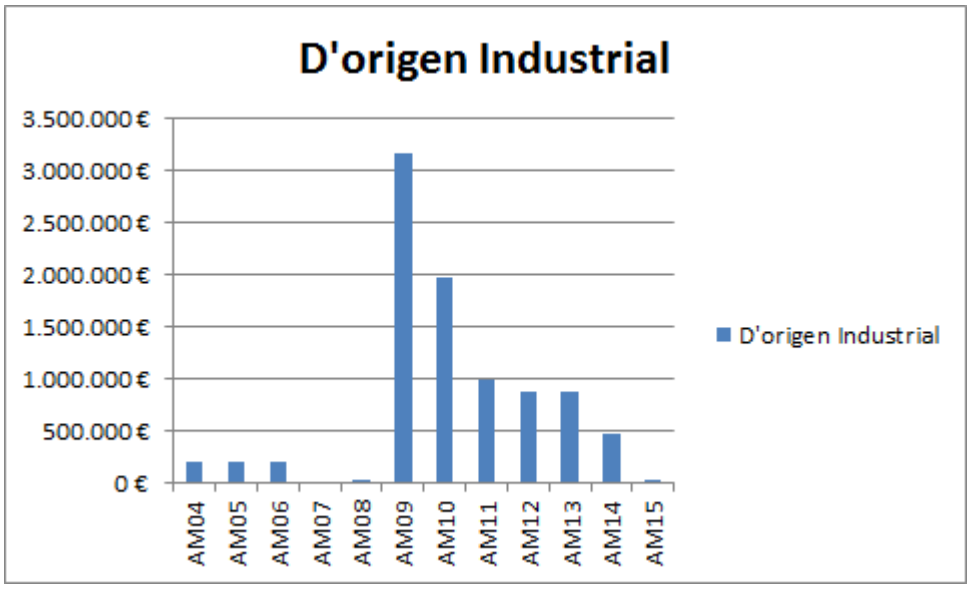
4.5.2 Amenaces

Pel que fa a les amenaces, es classifiquen en quatre grups diferents.
Primerament en el grup de desastres naturals, on la probabilitat és molt baixa i per tant el risc també ho és.

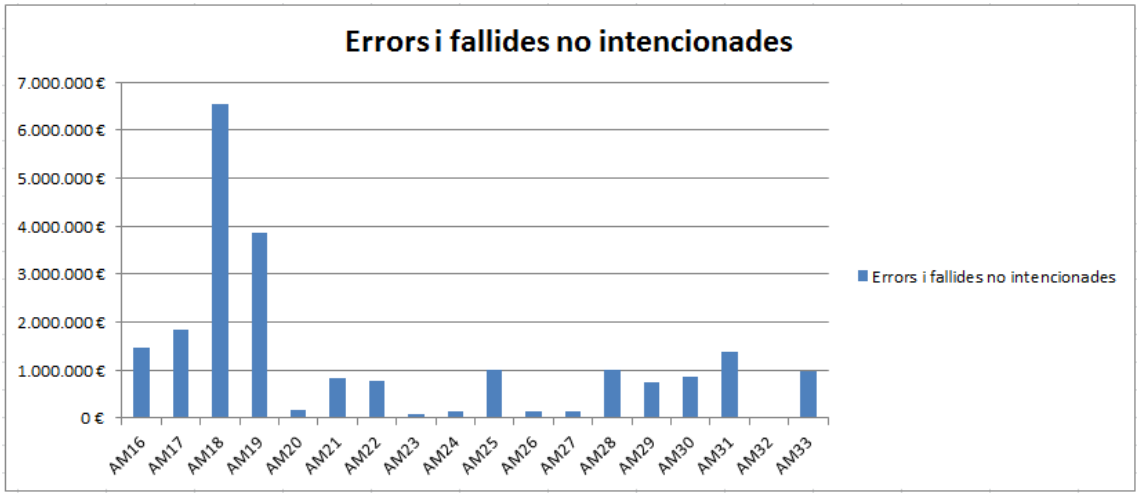


En la segona classificació, les amenaces d'origen industrial, en destaca una per sobre de la resta i és l'averia física o lògica. És normal ja que en el hardware i les aplicacions és on està el negoci de l'empresa. La segueix el tall de subministraments, ja que sense subministraments no es pot donar servei i no es pot fer funcionar el CPD. En aquest cas, la freqüència disminueix bastant no perquè no és donin força talls de subministrament, sinó perquè tots els equips

funcionen amb SAIs i està tot redundat. Per tant, s'està contemplant talls curts de subministrament. En cas que el tall fos molt llarg i les bateries dels SAIs s'esgotessin, si que hi hauria un risc molt més alt.



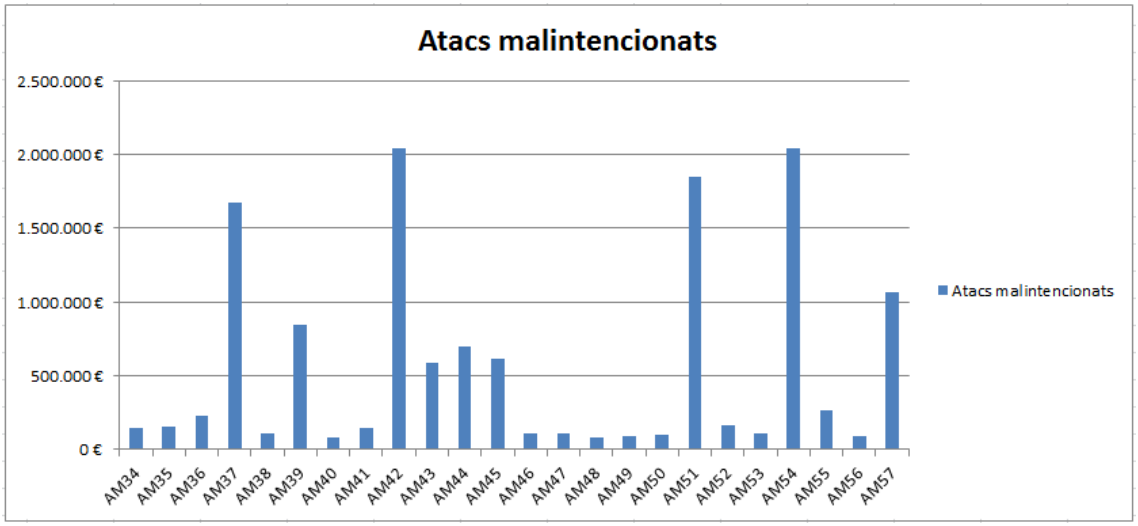
La següent classificació fa referència als errors o a les fallides no intencionades i destaca la amenaça en els errors de monitorització. El fet que hi hagi errors de monitorització, donat que hi ha un CPD que controlar, pot generar molts problemes als tècnics, o bé per falsos positius o bé per falsos negatius a l'hora de saber si els sistemes estan funcionant correctament o no. Els errors de configuració també son una gran amenaça, ja que són complicats de detectar i porten temps per solucionar-ho, i si algun aparell principal es veu afectat per una mala configuració pot deixar a l'empresa sense servei.



En la última classificació, els atacs malintencionats, hi ha quatre amenaces destacades:

- Abús de privilegis d'accés
- Accés no autoritzat
- Denegació de servei
- Ocupació enemiga

Son les principals amenaces ja que poden fer molt de mal a la organització.



Finalment, les amenaces més perilloses per l'organització són les següents:

AM18	Errors de monitorització			X		X	17.930,50 l	6.544.633 l
AM19	Errors de configuració			X			10.105,44 l	3.688.486 l
AM09	Averia d'origen físic o lògic				X		8.665,01 l	3.162.729 l
AM42	Accés no autoritzat		X	X			5.584,68 l	2.038.408 l
AM54	Ocupació enemiga		X		X		5.584,68 l	2.038.408 l

L'amenaça que contempla el risc més elevat el la dels errors de monitorització. Aquesta amenaça te un gran risc degut a que afecta principalment al CPD i als serveis del clients, actius més importants de l'empresa. Si hi ha una mala monitorització i no avisa dels errors o per contra dóna falsos positius, es poden veure afectats els sistemes del CPD.

Seguidament, una de les amenaces més critiques és la dels errors de configuració, ja que de la mateixa manera que en el punt anterior, una mala configuració en algun element del CPD pot afectar greument als serveis que s'ofereixen als clients.

Seguint en la mateixa línia, la disponibilitat de serveis dels clients, si hi ha una averia física o lògica en algun element, pot comportat seriosos problemes.

Finalment, les amenaces també amb risc elevat són les que impliquen accessos no autoritzats i ocupació enemiga als sistemes d'informació de l'empresa. Es podria fer molt de mal amb un mal ús de la informació o una eliminació d'aquesta.

5. Proposta de Projectes

A partir dels resultats obtinguts en el anàlisi de riscos, seguidament es plantegen varis projectes de millora per tal de disminuir el risc de les amenaces més importants en els actius més crítics. També és plantejaran projectes per tal d'optimitzar recursos i reduir costos.

5.1. Projecte 1 - Redundància externa de serveis

Taula Resum

	Contingut
Objectius	Donar redundància als equips que hi ha al CPD per poder garantir la disponibilitat dels serveis propis.
Riscos a mitigar	AM03, AM09, AM10, AM33, AM12, AM51
Controls afectat	12.3, 17.1, 17.2

Descripció

L'objectiu d'aquest projecte és reduir el risc de perdre disponibilitat en els serveis bàsics dels quals disposa l'empresa i tenen un alt valor pel negoci.

Es tracta de contractar un servir extern, a un altre ubicació geogràfica, i redundar aquelles màquines que siguin crítiques. En aquest cas, com redundar externament tots els serveis dels clients seria molt costos, només es redundaran les màquines virtuals que necessitin de disponibilitat total.

Extreien la informació de l'anàlisi de riscos, es redundaran les màquines virtuals que conten els següents sistemes:

- VM Correu Electronic
- VM de BBDD
- VM d'ERP
- VM de CRM

D'aquesta manera la informació estarà totalment sincronitzada en dos CDP ubicats en zones geogràfiques diferents. En cas d'haver una fallida en els sistemes, o una no disponibilitat del servei en el CPD propi, actuaria el CPD extern.
Tot això s'aconsegueix amb eines de VmWare, sistema de virtualització que ja utilitza l'empresa.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Manager IT: Negociació i contractació amb un proveïdor de hosting el host necessari per dur a terme el projecte.
- Responsable Sistemes i Xarxes: Definició del tipus de servidor o servidors que es contractaran i dels serveis que es necessitaran. També gestionarà les possibles parades en el servei durant la fase de migració.
- Administrador: S'encarregarà de gestionar la redundància de les màquines en ambdós CPDs. Configurarà la sincronització de les màquines i comprovarà que tot està funcionant correctament un cop finalitzada la migració.

Planificació

El projecte s'haurà de planificar per fases degut al gran volum d'informació que s'ha de moure. En cada fase es mourà una de les VM cap al CPD extern. Les actuacions es realitzaran en horaris no crítics per l'empresa, ja que implicarà la parada dels serveis durant el procés de migració, per tant, es realitzarà el cap de setmana o si donés temps suficient en alguna màquina en concret, durant la nit.

Pressupost

- Contractació d'un servidor capaç de executar les 4 màquines virtuals juntament amb un entorn de xarxa i capacitat de disc.

  881€/mes o 10.572€/any
- Llicencies VMware necessàries per la funcionalitat de redundància.

  1.200€
- Hores Manager IT

  10h x 40€/h = 400€
- Hores Responsable IT

  20h x 30€/h = 500€
- Hores Administrador

10h x 20€/h = 200€

- Hores Nocturnes Administrador

  30h x 30€/h = 900€

Total Pressupost: **3.200€ implantació i 10.572€ anuals**

5.2. Projecte 2 - Backups Externs

Taula Resum

	Contingut
Objectius	Externalitzar les còpies de seguretat per tal de tenir disponibilitat en cas que les copies locals no es poguessin utilitzar.
Riscos a mitigar	AM09, AM33, AM01, AM02, AM03
Controls afectat	12.3

Descripció

L'objectiu d'aquest projecte és reduir el risc enfront a la pèrdua de dades.

Es tracta de contractar un servei extern on poder ubicar les copies de seguretat. Actualment les copies de seguretat tant dels clients com dels propis sistemes es guarden dins de la mateixa ubicació geogràfica, ja que estan en servidors diferents, però dins del mateix CPD.

La finalitat es externalitzar aquesta informació fora per tal de poder recuperar-la en cas d'un greu problema al CPD o un possible incendi o inundació que destrossés els sistemes d'informació.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Responsable Sistemes i Xarxes: Negociació i contractació amb un proveïdor de Backup el servei necessari per dur a terme el projecte.
- Administrador: S'encarregarà de gestionar les copies de seguretat i de configurar-les.

Planificació

La planificació del projecte és de termini immediat, ja que el que s'ha de fer és trobar un proveïdor que ofereixi aquest servei i negociar els costos. Un cop aconseguit s'haurà de decidir una política de copies de seguretat i implementar-la.

Pressupost

- Contractació del servei extern de copies amb capacitat de 2TB.

  650€/mes o 7.800€/any

- Hores Responsable IT

  5h x 30€/h = 150€

- Hores Administrador

  10h x 20€/h = 200€

Total Pressupost: **350€ implantació i 7.800€ anuals**

5.3. Projecte 3 - Condicionament CPD

Taula Resum

	Contingut
Objectius	Reforçar les mesures de seguretat i millorar els condicionaments de la part més important de l'empresa, el CPD
Riscos a mitigar	AM18, AM09, AM10, AM31, AM11, AM12, AM14
Controls afectat	11.1.1, 11.1.2, 11.2

Descripció

L'objectiu d'aquest projecte és reforçar les mesures de seguretat i millorar els condicionaments de la part més important de l'empresa, el CPD.

En primer lloc s'implantarà un sistema d'accés biomètric, de tal manera que només es podrà accedir al CPD amb l'empremta dactilar. D'aquesta manera ens assegurem que només pugui entrar al CPD qui realment tingui permisos i evitar la possibilitat de que algú robi o es trobi una targeta amb accés i pugui entrar sense ser identificat. A més, quedarà registre de l'hora exacta d'entrada i sortida, ja que per sortir del CPD també s'ha de fer servir l'empremta.

En segon lloc, es realitzarà una instal·lació de refrigeració per aire molt més robusta que l'actual. Actualment es refrigera el CPD amb un sol aparell d'aire fix i amb altres aparell mòbils coneguts com "pingüins". Per tant, aquest projecte contempla la refrigeració total del CPD amb aparell robustos i amb controls i alarmes de temperatura.

Finalment, com a última millora del CPD, s'implantarà un SAI centralitzat (a part dels que ja estan funcionant) de gran potencia, per donar continuïtat al funcionament del CPD en cas d'un tall de subministraments.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Manager IT: S'encarregarà de la gestió i negociació de la implantació i compra de serveis i productes. Decidirà juntament amb els responsable de Sistemes i el responsable de seguretat els models a implantar. També supervisarà amb el comitè de direcció els pressupostos per la implantació.
- Responsable Sistemes i Xarxes: Ajudarà al manager IT amb la cerca del model de sistema d'empremta digital més adient i supervisarà la implantació d'aquest.
- Responsable Seguretat: Ajudarà al manager IT amb la cerca del model de sistema de refrigeració i de SAIs més adients i supervisarà la implantació d'aquests.

- Administrador: S'encarregarà de la configuració i assignació de permisos del sistema d'accés per empremta dactilar. També realitzarà les comprovacions junt amb els responsables del bon funcionament de l'aire i els SAIs.
- Comitè Direcció: Supervisarà els costos i pressupostos de la implantació i prendrà la decisió final en quan a la implantació.

Planificació

La planificació del projecte és de termini mig, donada la dimensió del projecte i l'impacte sobre l'actiu que s'ha d'implantar. S'haurà de gestionar de manera que el CPD no deixi de funcionar i assegurar-se de realitzar les actuacions més crítiques en els horaris menys crítics.

Pressupost

- Contractació del servei + Instal·lació del sistema d'empremta dactilar.
  5.000€
- Contractació del servei + Instal·lació del sistema de refrigeració.
  4.500€
- Contractació del servei + Instal·lació del SAI centralitzat.
  8.000€
- Hores Manager IT
  40h x 40€/h = 1.600€
- Hores Responsable IT
  25h x 30€/h = 750€
- Hores Responsable Seguretat
  30h x 30€/h = 900€
- Hores Administrador
  10h x 20€/h = 200€
- Hores Comitè Direcció
  5h x 60€/h x 2 membres = 600€

Total Pressupost: **21.550€**

*Aquest cost és orientatiu i variarà en funció dels models que finalment s'implantin, les negociacions que s'aconsegueixin i el temps que finalment dediqui cada membre implicat.

5.4. Projecte 4 - Pla de redundància en els serveis TIC dels clients

Taula Resum

	Contingut
Objectius	Elaborar un nou producte per oferir als clients per tal d'assegurar la redundància i disponibilitat de la informació
Riscos a mitigar	AM03, AM09, AM10, AM33, AM12, AM51
Controls afectat	12.3, 17.1, 17.2

Descripció

L'objectiu d'aquest projecte és elaborar un nou producte per oferir als clients per tal d'assegurar la redundància i disponibilitat de la informació.

Un dels punts més crítics amb els que es troba l'empresa és que els serveis dels clients no estan redundats, i en cas d'una fallida en els sistemes o en el propi CPD només quedaria la opció de tirar de copies de seguretat. Suposant que no es tracta d'un desastre, no es perdria la informació gracies a les copies de seguretat, però si que hi hauria un temps d'inactivitat fins tornar a poder oferir el servei.

L'objectiu d'aquest projecte és desenvolupar una nova via de negoci en la qual poder oferir als clients un millor servei. Aquest servei consistirà en la redundància dels serveis en un CPD extern, de la mateixa manera que es realitzarà en un dels projectes anteriorment comentats amb els propis sistemes de l'empresa.

Aquest projecte contempla tant la millora en la seguretat dels clients, actiu més crític de l'empresa, com la tranquil·litat legal de haver advertit als clients de les conseqüències que pot tenir no contractar aquest nou servei. A part, al ser un nou producte que llençar al mercat, també és una nova via de negoci per fer créixer l'empresa.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Manager IT: Negociació amb un proveïdor de hosting el host/s necessari/s per tal de fer una valoració de costos.
- Manager Comercial: Elaboració del model de venta i màrqueting del nou producte. Realització de la campanya comercial per tal de forçar i convèncer als clients a contractar el nou producte.
- Manager Administratiu: Valoració del preu al qual s'ha de vendre el nou producte en funció dels costos negociats pel Manager IT.

- Tècnic Comercial: Ajudar amb la campanya comercial portada a terme pel Manager Comercial.
- Responsable IT: Aportacions tècniques a tenir en compte i direcció i aplicació del producte en els clients que ho contractin.
- Comitè Direcció: Supervisarà els costos i pressupostos de la implantació, valorar i decidir si es un bon model de negoci i prendrà la decisió final en quan a la implantació i comercialització d'aquest.

Planificació

La planificació del projecte és de termini curt, principalment perquè és un nou model de negoci amb el qual es guanya tant en seguretat, com en tranquil·litat i també econòmicament a part de que s'ofereix un servei de qualitat als clients que ho vulguin.

Pressupost

- Contractació d'un servidor capaç de executar les màquines virtuals dels clients juntament amb un entorn de xarxa i capacitat de disc.
  Entre 881€/mes i 16.000€/mes en funció els clients que contractin el servei.
- Llicencies VMware necessàries per la funcionalitat de redundància.
  1.200€ i 24.000€ en funció els clients que contractin el servei.
- Hores Manager IT
  30h x 40€/h = 1.200€
- Hores Manager Comercial
  60h x 40€/h = 2.400€
- Hores Manager Administratiu
  20h x 40€/h = 800€
- Hores Responsable IT
  30h x 30€/h = 900€
- Hores Tècnic Comercial
  40h x 12€/h = 480€
- Hores Comitè Direcció
  10h x 60€/h x 2 membres = 1.200€

Total Pressupost: **6.980€**

*En aquest pressupost només es contemplen els costos del personal. El cost del servei no es contempla ja que es contractarà en funció els clients contractin el producte, i el cost del servei amortitzarà els costos de contractació.

5.5. Projecte 5 - Implantació IDS

Taula Resum

	Contingut
Objectius	Implantat un sistema IDS enfront a amenaces i software malintencionat.
Riscos a mitigar	AM18, AM42, AM54, AM51, AM37, AM39,
Controls afectat	12.2, 12.4, 12.6, 12.7

Descripció

L'objectiu d'aquest projecte és implantat un sistema IDS enfront a amenaces i software malintencionat.

S'implantarà us sistema que monitoritzi la xarxa de l'empresa i ajudi a identificar qualsevol amenaça del tipus malware que pugui provocar pèrdua d'informació o pèrdua de disponibilitat en els serveis.

El sistema que s'implantarà serà Snort juntament amb el seu paquet de gestió i monitorització web anomenat Sonrby. Es configuraran alertes via mail per les deteccions de paquets sospitosos.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Responsable Sistemes i Xarxes: Supervisió i direcció del projecte.
- Administrador: S'encarregarà de la implantació i la posterior gestió del sistema.
- Tècnic IT: suport en la implantació i gestió de les notificacions.

Planificació

La planificació del projecte és de termini curt, ja que una de les principals amenaces que afecten a l'empresa són les fallades en la monitorització. Amb aquest sistema s'aconseguirà millorar el sistema de monitorització i donada la criticitat de l'amenaça és important implantar-ho de manera quasi immediata.

Pressupost

- Contractació del sistema Snort i Snorby.

  0€ És un sistema opensource i per tant no te cost de llicències.

- Hores Responsable IT

  10h x 30€/h = 300€

- Hores Administrador

  80h x 20€/h = 1.600€

- Hores Tècnic IT:

  40h x 12€/h x 2 membres = 960€

Total Pressupost: **2.860€**

5.6. Projecte 6 - Pla de continuïtat del negoci

Taula Resum

	Contingut
Objectius	Definir el pla d'actuació enfront a possibles escenaris crítics.
Riscos a mitigar	AM33
Controls afectat	6.1.3, 12.2, 12.3, 17.1

Descripció

Un element fonamental a l'hora d'assegurar i preservar els processos de negoci crítics de l'Empresa és disposar d'un Pla de Continuïtat que estableixi de forma clara i precisa com s'ha d'actuar i què s'ha de fer quan les mesures de seguretat implantades no han pogut frenar la materialització d'un risc.

Mitjançant un Pla de Continuïtat l'organització intentarà minimitzar el temps d'inactivitat si es produeixen aquestes interrupcions.

Aquest pla de continuïtat serà una guia de com actuar en cas de que alguns elements vitals de l'empresa fallin. El pla de continuïtat estarà basat en la metodologia ITIL v3.

Dins del pla es contemplarà tenir servidors de backup al magatzem i les copies actualitzades de manera que el la reanudació d'un sistema no sigui crític. Dins d'aquest pla també es tenen en compte els projectes anteriorment comentats com el de la redundància externa dels sistemes i els backups externs.

Aquest pla definirà quins seran els processos i els plans a seguir en funció hagi d'entrar en funcionament un els dels servidors externs o s'hagin de fer servir les copies externes o internes de l'empresa.

El pla també guiarà els processos en funció del impacte. És a dir, es contemplaran varis escenaris, principalment els més crítics, i s'elaborarà un pla d'actuació. Aquest projecte serà constantment actualitzat amb millores i nous conceptes de resolució d'incidències.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Manager IT: Serà la persona responsable de dirigir el projecte i de reunir-se amb totes les parts implicades en la seguretat de l'empresa per tal de redactar els procediments necessaris en cada àmbit de l'empresa.
- Responsable Programari: S'encarregarà de redactar i ajudar al Manager IT amb la elaboració de procediments enfront a la part software.

- Responsable IT: S'encarregarà de redactar i ajudar al Manager IT amb la elaboració de procediments enfront a la part IT.
- Responsable Seguretat: S'encarregarà de redactar i ajudar al Manager IT amb la elaboració de procediments enfront a la part de seguretat i maquinaria.
- Comitè direcció: Supervisarà els procediments establerts i donarà l'acceptació d'aquests.
- Tècnics: Aportaran informació al Manager IT de la experiència de les incidències més comuns, l'experiència en la seva resolució i altres detalls i factors a tenir en compte.

Planificació

La planificació del projecte és de termini llarg. Donada la magnitud del projecte, es contempla un projecta a llarg termini ja que s'han de tenir moltes coses en compte, és necessiten moltes reunions, moltes sensacions i detalls per afinar en els escenaris i la seva resolució. A més serà un projecte en constant actualització ja que dia a dia sorgeixen nous problemes i noves situacions.

Pressupost

- Hores Manager IT

  180h x 40€/h = 7.200€
- Hores Responsable IT

  40h x 30€/h = 1.200€
- Hores Responsable Programari

  20h x 30€/h = 600€
- Hores Responsable Seguretat

  20h x 30€/h = 600€
- Hores Comitè direcció

  10h x 60€/h x 2 membres = 1.200€
- Hores Tècnics

  10h x 12€/h x 5 membres= 600€

Total Pressupost: **11.400€**

5.7. Projecte 7 - Mitigació Malware

Taula Resum

	Contingut
Objectius	Reduir la possibilitat de malware a la organització.
Riscos a mitigar	AM42, AM54, AM37, AM39, AM21, AM36, AM51, AM33, AM35, AM27, AM53
Controls afectat	12.2.1

Descripció

Per tal de mitigar malware a l'organització, s'aplicaran varies millores.

Primerament s'aplicarà una política d'actualització d'antivirus. La gran majoria d'infeccions venen donades per l'execució de software maligne per part dels usuaris connectats a la xarxa. Per tal de reduir d'incursió de malware a l'empresa serà necessari tenir els antivirus actualitzats amb una antiguitat màxima de 3 dies abans de poder accedir a qualsevol recurs en xarxa de l'empresa.

En segon lloc, s'aplicaran polítiques de seguretat a l'active directory de l'organització, per tal d'impedir l'execució per part de l'usuari de certs software coneguts com a malware.

Finalment, i donat que és un dels virus més potents que hi ha, es designarà una política de seguretat a l'AD per tal de reduir o eliminar l'impacte del virus conegut com Cryptolocker. Aquesta política consistirà en evitar que un arxiu pugui canviar la seva extensió a .encrypted, atac principal que realitza el cryptolocker, xifrar tots els arxius i posar l'extensió .encrypted.

A part de tot això es realitzaran algunes jornades d'informació, conscienciació i formació als usuaris enfront a aquestes situacions i enfront a la recepció de correus electrònics sospitosos.

Personal implicat

El personal implicat i les tasques a realitzar en aquest projecte serà:

- Responsable Sistemes i Xarxes: Supervisió i direcció del projecte. Impartir les jornades de formació i conscienciació als usuaris
- Administrador: S'encarregarà de la implantació i configuració de les diferents polítiques de seguretat i de les actualitzacions dels antivirus.
- Tècnic IT: Assegurar que els equips dels usuaris tenen els antivirus correctament configurats i conscienciar als usuaris de la perillositat del malware.

Planificació

La planificació del projecte és de termini curt, ja que no és un projecte de massa dificultat i pot aportar molts beneficis a la empresa.

Pressupost

- Hores Responsable IT

  5h x 30€/h = 150€
- Hores Administrador

  20h x 20€/h = 400€
- Hores Tècnic IT:

  10h x 12€/h x 2 membres = 240€

Total Pressupost: **790€**

5.8. Planificació

Projecte	Duració	Començament	Fi
Backups Externs	1 mes	Juliol 2015	Agost 2015
Redundància externa de serveis	2 mesos	Agost 2015	Octubre 2015
Pla de redundància en els serveis TIC dels clients	6 mesos	Setembre 2015	Març 2016
Condicionament CPD	3 mesos	Setembre 2015	Desembre 2015
Mitigació Malware	1 mes	Juliol 2015	Agost 2015
Implantació IDS	3 mesos	Gener 2016	Març 2016
Pla de continuïtat del negoci	Constant	Setembre 2015	Constantment en millora

Primerament es planificarà la implantació dels Backups Externs, ja que es dels projectes més assequibles d'implantar i dels que més valor aportaran a l'empresa. A la mateixa vegada també es començarà a implantar el projecte de mitigació de Malware, ja que no implicarà un gran cost econòmic ni de recursos.

Un cop finalitzada la implantació dels Backups es procedirà a implantar la redundància externa de serveis i es contempla que això duri uns dos mesos. Durant la implantació d'això també es començarà a dur a terme el pla de redundància dels sistemes dels clients. En la fase en la que ens trobarem ja hi haurà prou coneixement per saber quin serà el proveïdor i quins seran els costos aproximats, per tant es podrà començar la campanya de marketing i venta del servei.

Donat que es un procés que els clients han d'anar contractant els serveis tindrà una extensió de 6 mesos en la primera campanya.

Al setembre del 2015, mentre s'està començant a realitzar la campanya de venta del servei, es procedirà a realitzar la millora del CPD, projecte que durarà uns 3 mesos aproximadament.

Al Gener de 2016 amb la majoria de projectes implantats, es centraran els recursos en la implantació d'un sistema IDS que ajudarà a detectar fallades de seguretat i millorar una de les principals amenaces de l'empresa, les fallades en la monitorització.

Finalment al Setembre del 2015 es començarà a implantar el projecte del pla de continuïtat del negoci. Aquest projecte estarà en constant evolució de millora, ja que a mesura que es vagin incorporant processos i clients s'haurà d'anar adaptant.

6. Auditoria de Compliment

Data Auditoria

Dimecres, 6 de Juny de 2016, Mataró.

Organització

L'auditoria es realitza a l'Empresa XX, SL, a les seves instal·lacions de Mataró.

Equip Auditor

L'auditoria serà realitzada per Esteban Sardanyés, membre intern de la plantilla de l'empresa.

Objectiu

L'objectiu de l'auditoria de compliment és valorar el nivell compliment de controls de seguretats definits en la norma 27002. Després de la implantació del SGSI i un cop aplicats tots els projectes de millora, es realitza aquesta auditoria per comprovar quins controls s'estan complint i a quin nivell.

Abast

L'abast de la auditoria es per tot el SGSI establert i amb la millora de projectes aplicats. Tal com és va definir al SGSI, l'abast del projecte afecta a tota la organització en nivell de seguretat informàtic. L'abast és tant a nivell corporatiu com a nivell de prestació de serveis a clients.

Metodologia

La metodologia emprada està basada en el model de maduresa de la capacitat, on es defineixen sis nivells per mesurar el nivell d'implantació dels controls definits per la norma 27002.

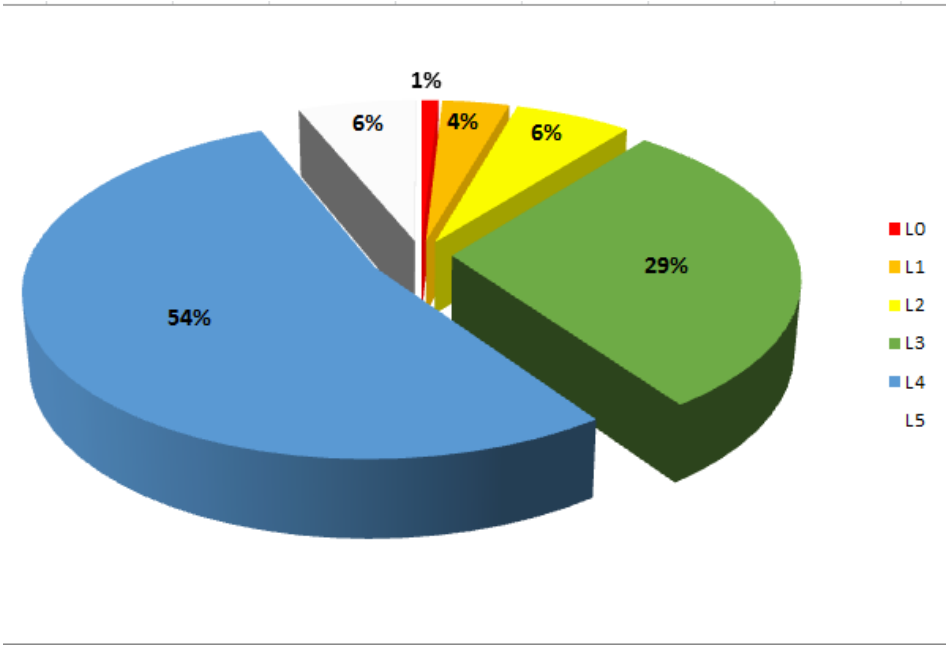
EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	**L0**	Inexistent	Carència completa de qualsevol procés que reconeguem. No s'ha reconegut que existeixi cap problema a resoldre.
10%	**L1**	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. 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 i 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.

Presentació de resultats

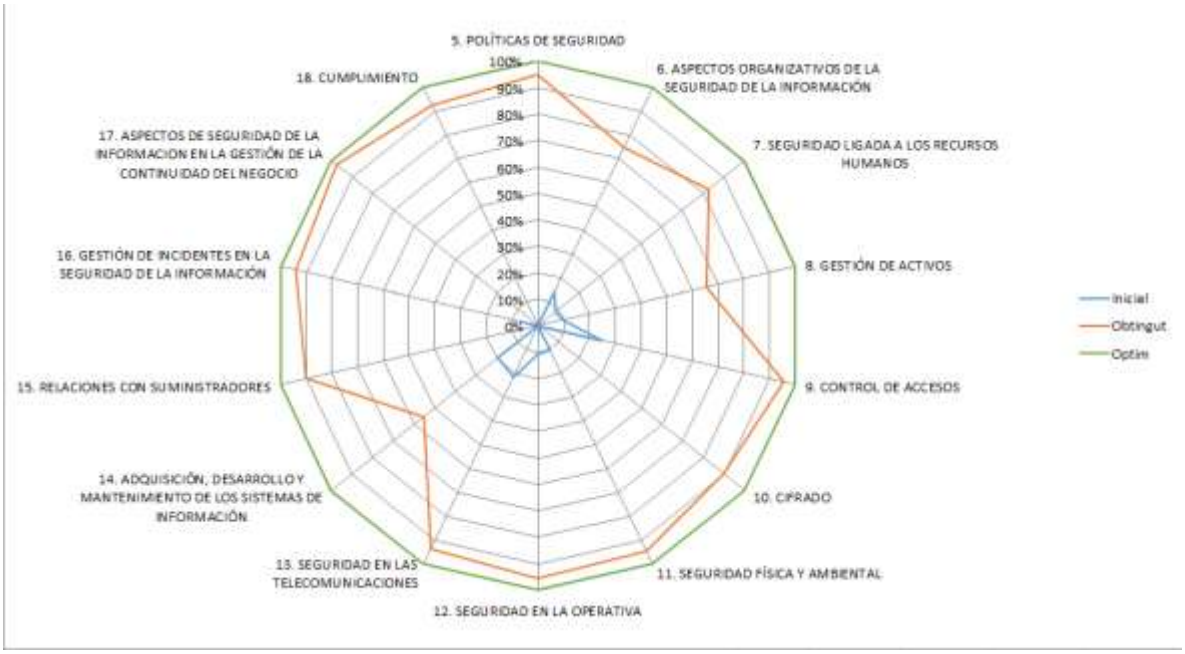
A continuació es mostren els resultats obtinguts de l'auditoria.

Primerament es mostra una taula on es pot observar el nivell en % del compliment òptim dels controls de seguretat basats en las norma 27002:2013. S'observa tant el nivell incial, abans d'aplicar el SGSI, com el obtingut un cop implantat el SGSI.

	Inicial	Obtingut
5. POLÍTICAS DE SEGURIDAD	0%	95%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	14%	75%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	8%	83%
8. GESTIÓN DE ACTIVOS	10%	65%
9. CONTROL DE ACCESOS	25%	96%
10. CIFRADO	0%	90%
11. SEGURIDAD FÍSICA Y AMBIENTAL	10%	95%
12. SEGURIDAD EN LA OPERATIVA	11%	96%
13. SEGURIDAD EN LAS TELECOMUNICACIONES	21%	94%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	19%	55%
15. RELACIONES CON SUMINISTRADORES	0%	90%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	7%	94%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0%	98%
18. CUMPLIMIENTO	0%	93%



Per veureu més gràficament es mostra el següent diagrama, on es poden observar els tres nivell, l'inicial, l'obtingut i l'òptim.



Tot el contingut detallat dels controls aplicats es pot trobar al arxiu adjunt al projecte "AuditoriaCompliment_F5.xls".

Per tal de poder dur a terme l'auditoria s'han realitzat una sèrie de taques:

- Entrevistes amb el personal de l'empresa.
- Reunions amb l'equip implicat.
- Anàlisi de les polítiques.
- Avaluació dels projectes implantats.
- Avaluació d'evidències obtingudes per part de la empresa.

6.1 No conformitats

Finalment, després d'avaluar i auditar el SGSI implantat, s'han extret una sèrie de no conformitats i observacions que es detallen a continuació.

	No Conformitat Menor	No Conformitat Major	Observacions
5. POLÍTICAS DE SEGURIDAD	0	0	0
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	1	0	1
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	2	0	0
8. GESTIÓN DE ACTIVOS	4	0	0
9. CONTROL DE ACCESOS	0	0	0
10. CIFRADO	0	0	0
11. SEGURIDAD FÍSICA Y AMBIENTAL	0	0	1
12. SEGURIDAD EN LA OPERATIVA	0	0	0
13. SEGURIDAD EN LAS TELECOMUNICACIONES	0	0	0
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	3	1	0
15. RELACIONES CON SUMINISTRADORES	0	0	1
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	0	0	0
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	0	0
18. CUMPLIMIENTO	0	0	0

Resum

Tal com indica el diagrama, els punts amb menys compliment dels controls són el 6, 8 i 14.

De tots, el que compte amb menys conformitat és el punt 14, "Adquisició, desenvolupament i manteniment dels sistemes de informació.", sobretot en el que representa la part de software.

La major no conformitat és la que fa referencia a que no hi ha cap política definida pel desenvolupament de software segur. Cada tècnic gestiona la seguretat a la seva manera.

En el apartat d'observacions, no s'han contemplat com No Conformitats perquè no suposen un ús específic de l'empresa i s'ha considerat que no afectava directament a la seguretat, però que es podria millorar.

No Conformitats

	No Conformitat nº 1
Tipus	No existeix la política
Control	6.2.1 Política de uso de dispositivos para movilidad.
Detall	No existeix cap política d'us per a dispositius portables. Tampoc es controlen les dades que es porten als dispositius mòbils i portàtils.
Tipus No Conformitat	No Conformitat Menor
Evidencia	Es van revisar les polítiques de seguretat de l'empresa i no hi ha cap que fagi referencia al ús de dispositius mòbils. També es van examinar alguns terminals i cap d'ells utilitzava antivirus ni bloqueig amb codi del terminal.
Recomanació	S'hauria de definir una política clara en la qual es faci constar que tots el terminals han de tenir un codi d'accés personal, un antivirus instal·lat (en el cas dels androids) i que no contenen informació confidencial de l'empresa, més enllà del correu.

	No Conformitat nº 2
Tipus	No existeix cap procediment
Control	7.2.1 Responsabilidades de gestión.
Detall	No hi ha cap procediment establert per que terceres parts apliquin les polítiques de seguretat de l'empresa
Tipus No Conformitat	No Conformitat Menor
Evidencia	Revisant els contractes amb la subcontractació de tercers, no es va trobar cap evidencia de que aquests es comprometin a treballar certificats per la ISO 27001, i tampoc que es comprometin a aplicar les mesures de seguretat exigides per l'empresa.
Recomanació	S'ha de desenvolupar un procés per tal d'exigir als tercers que es comprometin a treballar amb les mesures de seguretat que demana l'empresa i fer-ho constar. També s'haurà de revisar que l'empresa compleix exigint auditories cada cert temps en funció de l'activitat del tercer.

	No Conformitat nº 3
Tipus	No existeix cap procés
Control	7.2.2 Concienciación, educación y capacitación en segur. de la informac.
Detall	Hi ha un procés de educació per al personal de l'empresa, però no hi ha cap aplicat per tercers
Tipus No Conformitat	No Conformitat Menor
Evidencia	Tot i que hi ha un procés aplicat a l'empresa per la formació i conscienciació del personal intern, no hi ha cap tipus de formació i conscienciació a tercers.
Recomanació	S'ha d'exigir als tercers que disposin d'una certificació ISO 27001, o en el seu defecte (segons les dimensions del tercer) formar-lo i conscienciar-lo de la manera de treballar amb la informació per tal de garantir la seguretat.

	No Conformitat nº 4
Tipus	No existeix la política
Control	8.1.3 Uso aceptable de los activos.
Detall	No hi ha establerta cap política ni cap control sobre el ús dels actius per part del personal.
Tipus No Conformitat	No Conformitat Menor
Evidencia	S'han trobat varis equips portàtils de treballadors amb software personals instal·lats, com "Hoffman" (Software per edició d'àlbums de fotografies) i alguns altres crackejats.
Recomanació	S'ha de definir una política d'ús dels equips personals i aplicar un control per garantir que als equips no s'instal·len softwares pirates ni software que no tinguis cap relació amb l'activitat a desenvolupar.

	No Conformitat nº 5
Tipus	No existeix cap procés de control
Control	8.3.1 Gestión de soportes extraíbles
Detall	Tots els equips de l'empresa disposen de ports USB i una gran majoria d'unitats de DVD. No existeix cap control per tal de saber la informació que es pot extreure de l'empresa.
Tipus No Conformitat	No Conformitat Menor
Evidencia	S'ha detectat que alguns USB del personal tenen software i documents de l'empresa, per tant, no hi ha cap control de que el personal pugui extreure informació.
Recomanació	S'hauria d'implementar un control i establir un procés per tal de limitar i controlar l'extracció d'informació.

	No Conformitat nº 6
Tipus	No existeix cap procés de control
Control	8.3.2 Eliminación de soportes.
Detall	No es té en compte si s'eliminen els medis extraibles un cop ja utilitzats. Només s'eliminen documents en paper de caràcter confidencial
Tipus No Conformitat	No Conformitat Menor
Evidencia	S'han trobat varis DVD i USBs amb informació confidencial de l'empresa guardats i els quals no estaven ni etiquetats ni controlats.
Recomanació	S'hauria d'aplicar una política de destrucció de suports que continguin informació confidencial una vegada ja no s'hagin d'utilitzar.

	No Conformitat nº 7
Tipus	No existeix cap politica
Control	8.3.3 Soportes físicos en tránsito
Detall	No hi ha definida cap politica per l'enviament de dispositius amb informació confidencial.
Tipus No Conformitat	No Conformitat Menor
Evidencia	En les ocasions que s'han d'enviar DVDs o USBs a tercers, no s'utilitza cap protecció per l'accés a la informació.
Recomanació	Definir una política d'us en la qual s'obligui a enviar la informació xifrada, ja sigui en DVD o en USB. També s'haurà d'aplicar un control per tal de garantir que el procés es dur a terme correctament.

	No Conformitat nº 8
Tipus	No existeix cap procediment
Control	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas
Detall	No hi ha definit cap procediment per tal de tractar la informació que viatja per la xarxa pública.
Tipus No Conformitat	No Conformitat Menor
Evidencia	Tot i que la gran majoria del personal treballa amb correu ssl, no sempre s'utilitzen protocols segurs de navegació per accedir a algunes pagines on es penja informació de l'empresa.
Recomanació	Definir un procediment per tal de forçar a que les pàgines on s'ha d'accedir per penjar documentació sempre siguin per ssl o amb certificats.

	No Conformitat nº 9
Tipus	No existeix cap politica
Control	14.2.1 Política de desarrollo seguro de software.
Detall	No hi ha cap politica definida pel que fa al desenvolupament de software. Cada tècnic es responsable de la seguretat que aplica en les aplicacions. Tampoc hi ha control per comprovar la seguretat.
Tipus No Conformitat	No Conformitat Major
Evidencia	En les reunions amb els tècnics s'ha comentat que no segueixen cap protocol a l'hora de programar.
Recomanació	Definir una política de desenvolupament de software segur. Aplicar controls per garantir que s'aplica aquesta política i contractar empreses que testegin les aplicacions abans de posar-les en producció.

	No Conformitat nº 10
Tipus	No existeix cap procediment
Control	14.2.5 Uso de principios de ingeniería en protección de sistemas.
Detall	Es un procés que es dóna per suposat en els enginyers de l'empresa, però no hi ha cap control ni procés definit.
Tipus No Conformitat	No Conformitat Menor
Evidencia	En les reunions amb els tècnics s'ha comentat que no segueixen cap protocol a d'aplicar el principi d'enginyeria.
Recomanació	S'ha de definit un procés per aplicar el principi d'enginyeria en el projectes que es desenvolupen i en les tasques que es realitzen.

	No Conformitat nº 11
Tipus	No existeix cap proces
Control	14.3.1 Protección de los datos utilizados en pruebas.
Detall	No hi ha un procés definit. Cada usuari es responsable de la informació que utilitza en els escenaris de prova.
Tipus No Conformitat	No Conformitat Menor
Evidencia	S'han detectat informació real als entorns de prova, ja que en comptes d'inventar-se la informació s'utilitza la informació de les BBDD ja en producció.
Recomanació	S'ha de definir i aplicar un procés per tal de no utilitzar informació real als entorns de prova. Es poden inclús crear base de dades amb informació irreal per tal de dur a terme les proves.

Obsevacions

	Observació nº 1
Tipus	No existeix cap procés
Control	6.1.4 Contacto con grupos de interés especial.
Detall	Es realitzen consultes quan son necessàries i cadascú realitza les seves. No queda documentat ni hi ha cap política que ho reguli.
Tipus No Conformitat	Observació
Evidencia	En les reunions amb el personal s'ha comentat.
Recomanació	Seria interesant definir una politica per tal de d'optimitzar un procés de documentar i mirar de colaborar amb grups de suport.

	Observació nº 2
Tipus	No existeix cap procés
Control	11.2.4 Mantenimiento de los equipos.
Detall	S'han definit els processos de manteniment només dels equips més crítics de la empresa.
Tipus No Conformitat	Observació
Evidencia	Els processos només contemplen els equips crítics, però no els equips dels usuaris i els barebone.
Recomanació	Es podrien definir controls per tal de realitzar manteniments més periodics als PCs dels usuaris i els barebone

	Observació nº 3
Tipus	No existeix cap procés
Control	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
Detall	Hi ha un procés definit per supervisar la seguretat de tercers però no hi ha un control per garantir que s'està aplicant aquest procés
Tipus No Conformitat	Observació
Evidencia	En les reunions amb el personal, ningú controla que el procés es dugui a terme de manera correcte.
Recomanació	S'hauria d'anar revisant el procés amb la finalitat de garantir que els tercers apliquen la seguretat pertinent als seus serveis

7. Presentació de Resultats i entrega d'Informes

Un cop finalitzat el Pla director de seguretat de l'Organització, realitzada la implantació de projectes i acabada l'auditoria de compliment, es presenten els següents documents annexos on es fa un resum i una presentació de les conclusions. Els documents on estan reflectits els resultats són els següents:

- Resum executiu.
- Presentació de resultats en format PowerPoint.
- Presentació de resultats en format vídeo.

8. Conclusions

Com a resum final del projecte, es pot concloure que l'empresa ha donat un salt important en quan a la seguretat de la informació.

Amb la implantació del pla director l'empresa aconsegueix una fulla de ruta en front a incidents, millora molt en quan a disponibilitat de serveis i detecció de vulnerabilitats als sistemes.

Gracies a la implementació dels projectes també s'ha aconseguit obrir noves vies de negoci segures, que faran créixer l'empresa amb l'adquisició de nous clients importants. Es podran oferir unes garanties de servei i disponibilitat que moltes empreses de la competència no poden oferir. Amb aquestes millores, l'empresa es veu confiada per créixer i començar a absorbir clients importants que vulguin externalitzar la seva infraestructura informàtica.

També es conclou que amb algunes millores més que acabin de corregir les no conformitats, l'empresa podria realitzar una auditoria de certificació per tal d'obtenir la ISO 27001:2013 i donar un salt de qualitat en el mercat, podent-se diferenciar de moltes empreses de la competència i per poder oferir una major confiança als clients.

El pla director també ha servir per definir rols i responsabilitats en el personal. Ara, cada membre de la plantilla té molt clar quines son les seves tasques i les seves responsabilitats en quan a seguretat, estan molt més conscienciat i involucrat en el projecte.

També hi ha una persona encarregada de gestionar el SGSI i garantir que els controls i el processos implantats s'estan complint mitjançant el model PDCA.

Finalment, hi ha algunes millores que es podrien dur a terme per tal de millorar:

- Definir i implantar processos i controls per el desenvolupament de software segur. Donat que el desenvolupament de software no és l'activitat principal del negoci, és un àrea en la que no s'ha aprofundit tant i en la que no s'han destinat tants recursos com en altres àrees més importants. Amb el creixement de l'empresa, és un àrea que el vol explotar i per tant assegurar.
- Millorar la seguretat en els actius que fan referencia al personal de l'empresa, tant en portàtils com en smartphones. Limitar l'extracció de dades i forçar a treballar únicament amb VPN quan el personal es trobi fora de l'organització. Limitar també la informació que es duu en els terminals.
- Continuar amb formació permanent del personal enfront a la seguretat, per tal de garantir el nivell tècnic i de conscienciació esperat.

9. Bibliografia

Enllaç web sobre la ISO 27002

http://iso27000.es/iso27002.html

Enllaç web sobre implantacions de SGSI

http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/512_fase_2_hacer_implantar_el_plan_de_sgsi.html

Material SGSI de l'assignatura cursada a la UOC durant el semestre del 2013.

Contingut dels llibres "Metodologia de Anàlisis i Gestió de riscos MAGERIT".

10. Annexos

10.1. Annex 1 – Sistema de Gestió Documental

- **SardanesLobatoEsteban_A01_Politiques.pdf**
    - Política de Seguretat
    - Procediment d'Auditories Internes
    - Gestió d'indicadors
    - Procediment de Revisió per Direcció
    - Gestió de Rols i Responsabilitats
    - Metodologia d'Anàlisi de Riscos
    - Declaració d'Aplicabilitat

10.2. Annex 2 – Resum Executiu

- **SardanesLobatoEsteban_A02_Resum_Executiu.pdf**

  Document on figura el resum executiu del projecte.

10.3. Annex 3 – Fitxers Addicionals

Resum dels fitxers addicionals al projecte que es detallen a continuació:

- **SardanesLobatoEsteban_A03_01_Analisi_Diferencial_Declaracio_Aplicabilitat.xls**

  Document on s'especifiquen els controls aplicats per l'empresa abans de la implementació del SGSI, en la fase 1 (primera fulla del document) i on s'especifiquen el controls que són aplicables per l'empresa (segona fulla del document).

- **SardanesLobatoEsteban_A03_02_Analisi_Risc.xls**

  Document on s'especifiquen els actius de l'empresa, les amenaces i és fa un anàlisi de riscos de actius enfront amenaces.

- **SardanesLobatoEsteban_A03_03_Auditoria_Compliment.xls**

  Document on es detalla l'auditoria de compliment de l'empresa un cop implantat el Pla director.

- **SardanesLobatoEsteban_A03_04_Presentació_Digital.pdf**

  Document on es mostra en format resum la presentació del projecte.

- **SardanesLobatoEsteban_A03_05_Presentació_Video.mp4**

  Arxiu amb l'exposició visual i oral del projecte.