Desenvolupament i implantació d'un Pla Director de Seguretat basat en les normes ISO/IEC27001:2013 i ISO/IES27002:2013

Nom Estudiant: Patricia Borrego Rodríguez

Programa: Màster Inter-Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions

Nom Consultor: Arsenio Tortajada Gallego

Centre: Universitat Oberta de Catalunya

Data Lliurament: 12 DE DECEMBRE DE 2014

FITXA DEL TREBALL FINAL

Títol del treball:	*Desenvolupament i implantació d'un Pla Director de Seguretat basat en les normes ISO/IEC27001:2013 i ISO/IES27002:2013*
Nom de l'autor:	*Patricia Borrego Rodríguez*
Nom del consultor:	*Arsenio Tortajada Gallego*
Data de lliurament (mm/aaaa):	*12/2014*
Àrea del Treball Final:	*Sistemes de Gestió de la Seguretat*
Titulació:	Màster Inter-Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

Aquest projecte es desenvolupa com a Treball Final de Màster, dintre del marc dels estudis del Màster Inter-universitari en Seguretat de les Tecnologies de la Informació i la Comunicació i de l'especialització de Gestió i Auditoria de la Seguretat de la Informació.

L'objectiu d'aquest projecte és aplicar els coneixements assolits durant el màster per a establir les bases a l'hora de realitzar un Pla Director de Seguretat i implantar un Sistema de Gestió de la Seguretat de la Informació en una empresa real.

Un SGSI permet gestionar la seguretat de la informació d'una empresa mitjançant un procés sistemàtic, documentat i conegut per tota l'organització. Aquesta seguretat de la informació consisteix en la preservació de la seua confidencialitat, integritat i disponibilitat, així com dels sistemes implicats en el seu tractament.

Els estàndards en els que es basa el desenvolupament d'aquest SGSI són el ISO/IEC27001:2013 i el ISO/IEC27002:13.

La implantació del SGSI es realitza seguint el mètode del cicle PDCA o cicle de Deming que es basa en procés iteratiu de qualitat en quatre fases: Plan - Do - Check - Act. Mitjançant l'aplicació d'aquest mètode s'aconsegueix crear un SGSI dins un procés o cicle de millora continua.

L'empresa en la que s'ha basat aquest projecte és una empresa real, excepte pel nom. Aquesta organització proporciona serveis i solucions informàtiques i de telecomunicacions, emmarcats dins el sector de les TIC.

Abstract (in English, 250 words or less):

This project is developed as a Master Thesis, within the framework of the "Inter-University Master in Security of Information and Communications Technology" studies and the Management and Audit Information Security specialization.

The aim of this project is to apply the knowledge acquired during the Master to establish the basis to develop a Security Master Plan and implement an Information Security Management System in a real company.

An ISMS allows to manage a company's information security through a systematic and well-documented process, known by the entire organization. This information security involves the preservation of its confidentiality, integrity and availability, as well as the systems involved in its treatment.

The development of the ISMS is based on the Standards ISO/IEC27001:2013 and ISO/IEC27002:2013.

The establishment of this ISMS is performed following the PDCA or Deming cycle method, based on a four phase iterative quality process: Plan - Do - Check - Act. Applying this method, allows to create an ISMS within a continuous improvement cycle.

The project has been developed in a real company, except for the name. This organization provides computer and telecommunication services and solutions, framed within the ICT sector.

Paraules clau (entre 4 i 8):

Seguretat, Informació, Estàndard, SGSI, Pla, Director

Índex

1. Introducció

1.1 Context i justificació del Treball

Avui en dia, la informació que gestionen les empreses per a dur a terme els seus processos de negoci és, sense cap dubte, un dels seus actius més valuosos. La quantitat d'informació gestionada ha crescut de forma exponencial des que la utilització de les TIC forma part dels processos de negoci d'aquestes.

Encara que aquesta informació pot estar gestionada i emmagatzemada de diverses formes i amb formats diferents, en qualsevol de les seues presentacions, és absolutament fonamental que sigui tractada i protegida correctament.

Actualment, les empreses han assolit dita importància i com a conseqüència directa s'han adonat de la necessitat d'establir mecanismes que permetin gestionar la seua informació complint amb els requeriments legals vigents i que garanteixen la seua seguretat.

El desenvolupament d'un Pla Director de Seguretat basat en la norma de referència ISO/IEC27001:2013 i ISO/IEC27002:2013 i la seua implantació mitjançant un Sistema de Gestió de Seguretat de la Informació o SGSI, permet a les empreses determinar quin és el seu estat actual quant a Seguretat de la Informació i a partir d'aquest, especificar quines mesures de seguretat són les adequades per a protegir els seus actius contra les amenaces que poden afectar als seus processos de negoci.

A través d'aquest SGSI, aconseguirem integrar un procés de millora continua de la Seguretat de la Informació i implantar una cultura de seguretat en la forma de treballar de l'empresa i de gestionar els seus actius d'informació.

1.2 Objectius del Treball

L'objectiu general d'aquest Treball és establir les bases per a la realització d'un Pla Director de Seguretat en l'empresa objecte d'estudi, en aquest cas, l'Empresa X.
A partir d'aquest Pla Director de Seguretat, començarà la implantació progressiva d'un SGSI a l'Empresa X.

Mitjançant aquest treball es pretén millorar l'estat de Seguretat de la Informació de l'empresa i establir un procés de millora continua d'aquest.

Basant-nos en la norma de referència ISO/IEC27001:2013, els objectius específics d'aquest treball són:

- Analitzar la situació inicial quant a Seguretat de la Informació de l'empresa
- Desenvolupament del sistema de gestió documental del SGSI basat en la norma ISO/IEC27001:2013
- Realització d'una anàlisi de riscos que poden constituir una amenaça per als actius i processos de negoci de l'empresa
- Proposta de projecte de millora de l'estat de Seguretat de la Informació
- Realització d'una Auditoria de Compliment

1.3 Enfocament i mètode seguit

A l'hora d'abordar aquest projecte, l'empresa triada no disposa de cap sistema de gestió de la seguretat de la informació implantat. Els procediments de seguretat existents en el moment de començament del projecte no s'han implantat com a part d'un sistema de gestió de la seguretat de la informació ni d'un procés de millora continuada, sino com una mesura de seguretat puntual per a un propòsit concret.

Tenint com a punt de partida aquesta situació, l'estratègia triada és desenvolupar un Pla Director de Seguretat que permeti a l'empresa començar la implantació d'un SGSI amb l'objectiu de millorar la seguretat de la informació en tota l'organització i integrar en tots els seus processos de negoci els procediments adients per a consolidar la seguretat de la informació en l'empresa.

Es considera que aquesta estratègia és la més idònia ja que els actius d'informació en l'empresa objecte d'estudi no sols es troben materialitzats en equips informàtics i per tant abasten aspectes físics, lògics i humans dins l'Organització.

Com a mètode de treball, s'ha triat desenvolupar aquest SGSI basant-se en les normes ISO/IEC27001:2103 i ISO/IEC27002:2013, ja que són les que actualment tenen una major difusió i acceptació a nivell internacional.

- L'estàndard 27001 recull les especificacions per a implantar un SGSI i és la norma certificable.

- L'estàndard 27002 recull el codi de bones pràctiques en la gestió de la seguretat de la informació.

La implantació del SGSI es durà a terme utilitzant com a mètode el cicle PDCA o cicle de Deming. Inclòs i descrit en l'estàndard ISO27000. Aquest mètode es basa en procés iteratiu de qualitat en quatre fases:

- **P**lan: Estableix els objectius i processos necessaris per aconseguir els resultats esperats.
- **D**o: Implantació dels nous processos.

- **C**heck: Mesurament dels nous processos i comparació dels resultats obtinguts amb els esperats.
- **A**ct: Anàlisi de les diferències entre els resultats obtinguts i esperats per a conèixer les causes i plantejar millores.

1.4 Planificació del Treball

Aquest projecte està planificat en 6 fases diferents. Cadascuna d'elles desenvoluparà una part del procés d'implantació del SGSI.

Fase	Descripció	Entrega
1	Situació actual: Contextualització, objectius i anàlisi diferencial	**03/10/2014**
2	Sistema de Gestió Documental	**17/10/2014**
3	Anàlisi de Riscos	**07/11/2014**
4	Proposta de Projectes	**21/11/2014**
5	Auditoria de Compliment de la ISO/IEC27002:2013	**05/12/2014**
6	Presentació de Resultats i entrega d'Informes	**12/12/2014**

2. Situació actual: Contextualització, objectius i anàlisi diferencial

2.1 Enfoc i selecció de l'empresa objecte d'estudi.

L'empresa objecte d'aquest projecte, d'ara endavant Empresa X, és un proveïdor global de serveis i solucions informàtiques i de telecomunicacions emmarcats dins el sector de les TIC.

La seua oferta es dirigeix principalment a grans i mitjanes empreses i administració pública, i es centra en projectes amb una gran càrrega de contingut tecnològic i serveis d'alt nivell.

Creada en 1989 i especialitzada en gestió de serveis i infraestructures TI, implantació d'infraestructures tecnològiques i solucions per a centres de dades i comunicacions, així com en serveis de monitorització, administració i suport.

El seu objectiu principal és ajudar als seus clients a millorar la seua productivitat i els seus processos de negoci.

Els seus objectius empresarials són:

- Generar valor empresarial i aconseguir la màxima qualitat de servei per als seus clients.
- Crear confiança i satisfacció en clients, col·laboradors i proveïdors.
- Compromís amb l'entorn social.

Concepció empresarial:

- Autofinançament i independència.
- Reinversió dels profits generats.
- Creixement consolidat.
- Generació de valor afegit.
- Identificació del seu equip humà amb els objectius i cultura d'empresa.

Polítiques marc:

- Èmfasi en la qualitat i el servei.
- Adequació dels serveis al client.
- Oferta de solucions obertes i integrals.
- Atenció al client a la recerca de la seua fidelitat.
- Serietat i professionalitat dels serveis.

Les característiques generals de l'Empresa X són:

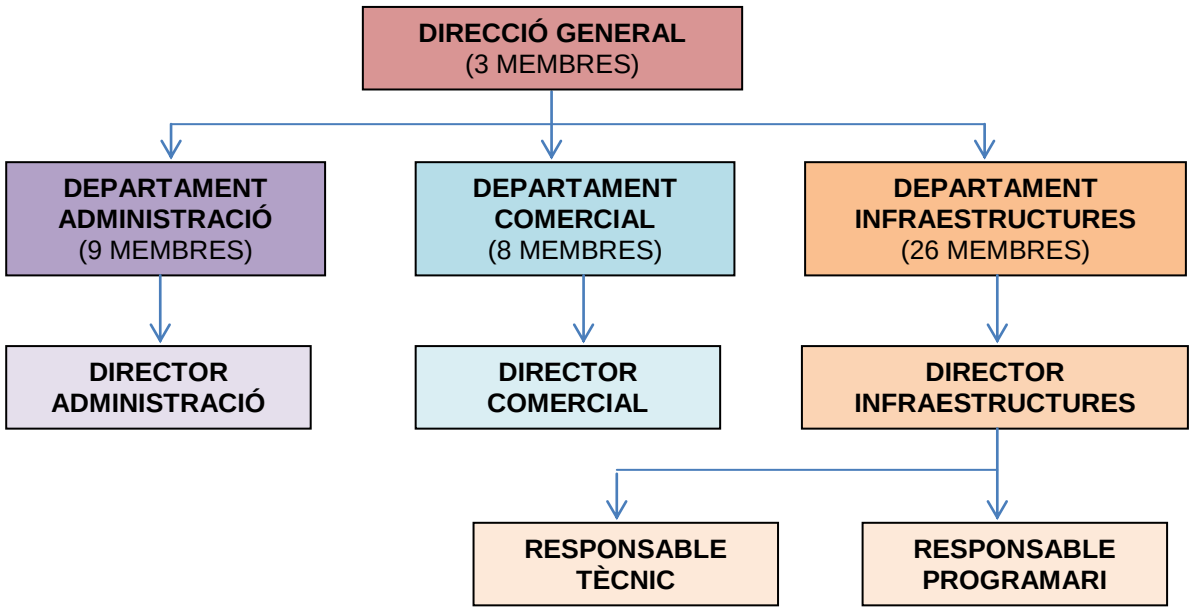
- Proporciona serveis de disseny i implantació d'infraestructures tecnològiques, comunicacions i centres de dates, així com serveis d'administració i suport de sistemes tant físics com virtualitzats.
- Els seus principals clients són empreses nacionals, de grandària variada, sobretot pimes i empreses grans així com administració pública.
- Les seues instal·lacions es troben en València capital.
- Actualment la seva plantilla consta d'uns 45 treballadors.

Encara que l'empresa no es dedica al desenvolupament d'eines informàtiques com a servei, el departament d'Administració utilitza un ERP propi per a gestionar la informació de clients, proveïdors, treballadors a més del procés de generació de nòmines i de facturació, entre d'altres.

Per altra banda, el departament de Comercial també empra aquesta mateixa eina ERP per a gestionar les comandes dels clients i les comandes que la pròpia empresa fa als seus proveïdors.

Per últim, el departament d'Infraestructures és l'encarregat de dur a terme els serveis contractats pels clients, ja sigui configurar i instal·lar tant serveis concrets com servidors, dominis o eines específiques. Aquests serveis es poden realitzar tant a les pròpies instal·lacions de l'Empresa X com a les instal·lacions dels clients, depenent del tipus de servei contractat pel client.

2.2 Organigrama de l'empresa



A continuació es proporciona una breu descripció de les diferents àrees o departaments que integren l'Empresa X.

Direcció General: Formada pels 3 membres executius de l'empresa que prenen les decisions estratègiques i finals a nivell corporatiu.

Departament Administració: Format pel Director d'Administració i 8 treballadors més. Aquest departament s'encarrega de tots els processos necessaris perquè l'empresa funcioni correctament en el seu dia a dia. Gestiona els processos relacionats amb Recursos Humans, Facturació, Nòmines, Viatges i Manteniment de les instal·lacions.

Departament Comercial: Format pel Director Comercial i 7 treballadors més. Aquest departament s'encarrega de la gestió de Clients i Proveïdors, estudis de viabilitat de futures Ofertes, Concursos i Comandes, així com de totes les accions relacionades amb Màrqueting i Publicitat de l'empresa.

Departament Infraestructures: Format pel Director d'Infraestructures i un equip de 25 persones. Dins aquest equip, existeixen 2 grups de treball:

Un grup format pel Responsable de Programari que coordina un equip de 4 persones que s'encarreguen del desenvolupament, gestió i manteniment de l'ERP propi de l'Empresa X.

Un grup format pel Responsable Tècnic que coordina un equip de 19 treballadors que desenvolupen la resta de serveis TIC que proporciona l'empresa als seus clients: instal·lació i configuració de diversos serveis, tasques de consultoria TIC, formació a clients, atenció al client i assistència telefònica, etc. A més, aquest grup de treball també gestiona la infraestructura pròpia de l'empresa i necessària per al seu funcionament diari, incloent-hi la infraestructura que dona suport a l'ERP intern.

2.3 Descripció de les Instal·lacions

Les instal·lacions de l'Empresa X es troben en un edifici d'oficines en el centre de la ciutat de València. Les oficines de l'empresa es troben situades en la tercera planta de l'edifici i ocupen la mitat de la planta aproximadament. Aquest centre de treball és la única seu que conforma l'empresa.

Quant a mesures de seguretat, l'edifici disposa de un conserge en la porta principal de l'edifici que s'encarrega de monitorar les càmeres de videovigilància distribuïdes per tots els passadissos i àrees comuns de l'edifici. El servei de consergeria de l'edifici és de 24 hores. No obstant això, l'empresa no disposa de càmeres de videovigilància dins les seues instal·lacions.

La porta d'accés únicament disposa d'una reixa de seguretat extensible i darrere d'aquesta hi ha una porta de cristall que dona accés directe a les oficines. Existeixen còpies de la clau que obri la reixa distribuïdes a diferents treballadors de l'empresa per tal que puguin accedir a les oficines tant en horari laboral com fora d'aquest si és necessari. Si un treballador intenta accedir a les oficines fora d'horari laboral el conserge de l'edifici pren nota del DNI del treballador i reté el document en consergeria fins que el treballador torna de l'oficina.

Les finestres que donen al pati interior de l'edifici tenen reixes instal·lades, mentre que les que donen al carrer no en tenen cap mesura de seguretat instal·lada.

L'empresa no disposa d'un servei d'alarma connectat a cap central d'alarmes o amb la policia.

Els despatxos dels directors es tanquen amb clau quan estan buits. Cada director té una còpia de la clau del seu despatx i a més en el departament d'Administració tenen còpia de totes les claus per obrir els despatxos en cas que sigui necessari.

El CPD o Centre de Processament de Dades, és la ubicació on es troba tota la infraestructura a nivell de comunicacions i servidors que l'empresa utilitza per desenvolupar les seues activitats de negoci. També es pot tancar amb clau però en horari laboral està obert habitualment. Tenen còpia de la clau d'accés tant el Responsable de Programari com el Responsable Tècnic a més del departament d'Administració.

Llevat els despatxos dels directors, la resta dels llocs de treball es troben distribuïts en un espai comú, agrupats per departaments o grups de treball i separats de l'àrea de Recepció per una armariada. Cada lloc de treball disposa d'una taula, una cadira, un telèfon connectat a la centraleta, un equip de sobretaula o portàtil, segons les necessitats, i una calaixera amb clau. La clau de cada calaixera està en poder del treballador que ocupa cada lloc de treball.

L'àrea de Recepció consta d'un lloc de treball de les mateixes característiques que els descrits abans i ocupat per un treballador del departament d'Administració. En aquesta àrea es troben també una tauleta amb informació corporativa i dues cadires que fan el paper de sala d'espera per a possibles visitants i clients.

Tota la documentació impresa es troba emmagatzemada en arxivadors que estan a l'abast de qualsevol persona que tingui accés a les instal·lacions de l'empresa.

Menjador, àrea amb microones, frigorífic, màquina de cafè i refrescos, i les facilitats necessàries perquè els treballadors puguin dinar, esmorzar, berenar ací: taules, cadires, coberts, etc.

El Magatzem té una porta amb clau d'accés que es guarda en el departament d'Administració.

2.4 Descripció Tècnica

Els recursos dels que disposa l'empresa per a desenvolupar les seues tasques es descriuen a continuació.

Existeix un sistema d'aire condicionat i calefacció centralitzat. Per aquest motiu, aquest sistema és insuficient per al CPD, sobretot als mesos de calor.

El CPD compta amb un SAI que proporciona una autonomia d'uns 30 minuts si es produeix un tall en el subministrament elèctric.

També en el CPD es disposa d'un extintor encara que és l'únic que hi ha en les oficines de l'empresa. La resta dels extintors es troben distribuïts pels passadissos de l'edifici d'oficines i no són propietat de l'Empresa X.

A continuació es dona una llista amb una breu descripció dels servidors ubicats al CPD de l'Empresa X. S'ha de tenir en compte que la gran majoria dels servidors estan creats i configurats en un entorn virtualitzat mitjançant VMWare ESX sobre una cabina de servidors físics HP Blade i un calaix HP de discos d'emmagatzemament compartit. Els servidors emprats en l'empresa són els següents:

- **2 Controladors de Domini**: Integrats en un mateix domini Active Directory sobre sistemes operatius Windows Server 2008 Standard. Encarregats de la validació dels treballadors en el domini corporatiu i del seu accés a la informació corporativa. També realitzen les tasques de servidors DNS i DHCP del domini.
- **Repositori de Dades**: Servidor inclòs en el domini corporatiu que proporciona accés a tota la informació dels diferents departaments. L'accés a aquesta informació es gestiona mitjançant els permisos dels usuaris de domini. Cada departament té accés a un directori comú on es troba la informació pròpia del departament. A banda, cada treballador té assignat un espai d'emmagatzematge propi dins el servidor i per últim, existeix un directori Públic on tots els treballadors de l'empresa poden accedir i on es comparteix informació no confidencial.
- **Servidor de Correu**: Servidor amb Windows Server 2008 Standard i Lotus Domino que gestiona el correu corporatiu.
- **Servidor de Correu Web**: Situat en la xarxa DMZ de l'empresa i amb IBM iNotes instal·lat i configurat.
- **Servidor de còpies de seguretat**: amb la eina HP Data Protector configurada per realitzar les còpies mitjançant una unitat de cintes externa HP i un pool de cintes LTO.
- **Servidor ERP Producció**: Servidor que executa l'eina ERP pròpia de l'empresa.

- **Servidor de Base de Dades**: Servidor on es troba la base de dades que empra el servidor ERP Producció i que emmagatzema tota la informació que es gestiona amb aquesta eina.
- **Servidor ERP Proves**: Servidor que executa l'entorn de proves de l'eina ERP. En aquest mateix servidor està configurada la base de dades de l'entorn de proves.
- **Centraleta telefònica**: Equip que executa el programari de gestió de la centraleta telefònica de l'empresa. La línia telefònica no està redundada.
- **Router** de connexió ADSL a Internet amb una única companyia. La connexió a Internet tampoc està redundada.
- **Antivirus Corporatiu**: Equip físic que gestiona l'aplicació centralitzada Trend Micro que permet administrar els antivirus de totes les màquines de l'empresa, tant si són equips d'usuari com servidors com màquines de proves.
- **Diversos servidors** Windows, Linux, Unix i HP-UX físics sense informació sensible, emprats per fer proves o donar formació a clients o interna, en cas necessari.
- **Proxy i Firewall**: Màquines físiques encarregades d'assegurar i monitorar les connexions d'entrada i eixida als recursos corporatius.

Tots els servidors tenen assignada una adreça IP estàtica.

Per altra banda, cada treballador té assignat un equip de treball amb les següents característiques bàsiques:

- Sistema operatiu Windows 7 Professional
- Inclosos en la xarxa i el domini corporatiu
- Adreça IP assignada de manera dinàmica pel servidor DHCP

A més es disposen d'equips d'usuari amb diversos sistemes operatius per realitzar proves i formació tant interna com a clients.
Existeixen 3 impressores i un escàner de documents en xarxa, a més d'una destructora de papers.

2.5 Definició dels objectius del Pla Director de Seguretat

Mitjançant aquest Pla Director de Seguretat l'Empresa X pretén determinar els projectes que han de ser escomesos a curt, mig i llarg termini per garantir una correcta gestió de la seguretat de la informació i evitar la materialització d'incidents de seguretat que podrien afectar a la mateixa.

Aquest Pla establirà l'itinerari a seguir per a implantar i gestionar els mecanismes de control necessaris que garanteixen que els riscos als que està exposada l'empresa són els que aquesta està disposada a assolir i no altres.

Com que aquesta serà la primera aproximació a la implantació d'un SGSI en l'Empresa X, l'abast d'aquest Pla Director de Seguretat inclou la gestió de la seguretat de tota la informació i els sistemes que la processen i suporten per al desenvolupament dels processos de negoci de l'Empresa X.

Els objectius establerts en aquest present Pla Director, aprovats i consensuats amb la Direcció General de l'Empresa X, són els següents:

- Avaluar i estimar el nivell de seguretat actual de la informació de l'empresa.
- Identificar els actius principals de l'empresa i establir la seua valoració.
- Analitzar i acotar els riscos als que estan exposats els actius de l'empresa.
- Definir i implantar els controls i mesures adients per garantir un nivell de seguretat de la informació adequat a les necessitats de l'empresa i protegir els seus actius i recursos.
- Establir i integrar un procediment de revisió periòdica i millora continuada de l'estat de la Seguretat de la Informació.

2.6 Anàlisi diferencial amb la norma ISO/IEC 27001:2013+ISO/IEC 27002:2013

L'objectiu de realitzar una anàlisi GAP o diferencial de la Seguretat de la Informació en l'Empresa X, es estimar l'estat inicial en el que es troba mitjançant l'avaluació dels controls implantats actualment amb respecte els controls necessaris no implantats, en relació amb la norma internacional ISO/IEC 27001 i ISO/IEC 27002.

La metodologia que s'emprarà està basada en el model SSE-CMM que defineix 6 nivells diferents, de 0 a 5, per a mesurar el grau d'implantació dels controls de seguretat.

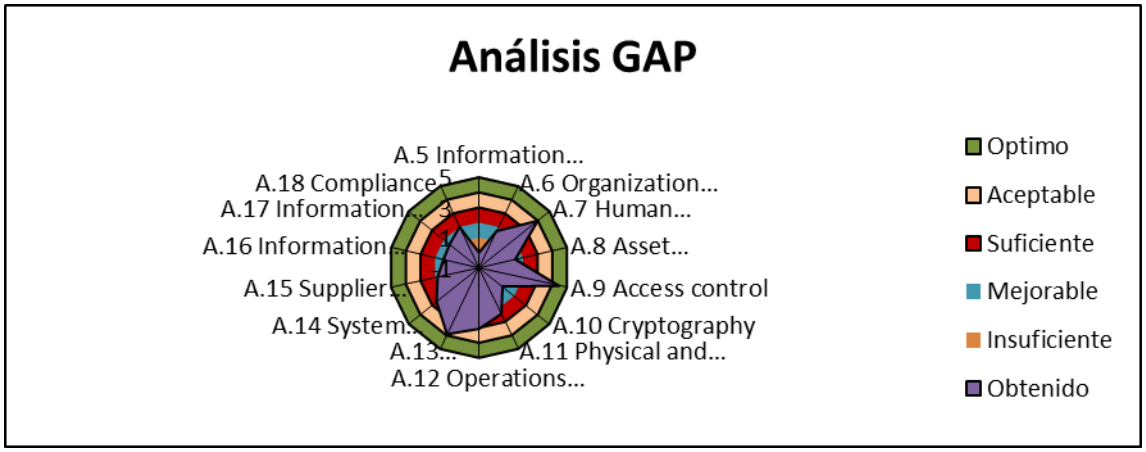
ID	NIVELL	PRÀCTIQUES DE GESTIÓ IT
0	**NO EXISTENT**	No hi ha una definició de responsabilitats en matèria de seguretat de la informació
1	**INICIAL** (hi ha una aproximació)	Les responsabilitats principals s'assignen o assumeixen informalment. Cada persona sap la seva responsabilitat, però no la dels altres.
2	**REPETIBLE** (existeix, amb moltes deficiències)	Se sap qui assumeix les funcions principals en matèria de seguretat de les TIC i de la resta del negoci, però les funcions de seguretat no estan definides ni documentades específicament, sinó que s'assumeixen individualment com a part d'altres funcions (per exemple, la direcció d'un projecte)
3	**DEFINIT** (existeix, amb algunes deficiències)	Les responsabilitats en seguretat de la informació s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, s'han donat a conèixer i s'ha fet o planificat la capacitació de totes les persones que ho requereixin
4	**GESTIONAT** (existeix i és correcte)	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, però no es fa una revisió anual per a verificar que totes les funcions s'han assignat bé i que els responsables desenvolupen la seva funció.
5	**OPTIMITZAT** (existeix i està integrada en un	Les responsabilitats s'han definit i documentat en tots els nivells de negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, es revisa

	cicle de millora continua)	periòdicament el desenvolupament d'aquestes funcions i hi ha un procés per a detectar deficiències en l'assignació i coordinació de funcions i per a aplicar-hi correccions

A continuació, podem veure un quadre resum de la maduresa dels controls implantats actualment a l'Empresa X junt amb la seua gràfica associada.

En l'arxiu Excel "BorregoRodriguez_GAP 27002_2013_TFM_Fase1.xls" es pot veure el desglossament de tots els controls avaluats en aquesta anàlisi diferencial.

	Valor
A.5 Information security policies	0
A.6 Organization of information security	1,7
A.7 Human resource security	4
A.8 Asset management	1,47
A.9 Access control	4,46
A.10 Cryptography	1
A.11 Physical and environmental security	2,42
A.12 Operations security	3,07
A.13 Communications security	3,92
A.14 System acquisition, development and maintenance	2,63
A.15 Supplier relationships	1,83
A.16 Information security incident management	1,43
A.17 Information security aspects of business continuity management	1,5
A.18 Compliance	2



3. Sistema de Gestió Documental

3.1 Política de Seguretat

La Direcció de Empresa X reconeix el rol de la Seguretat de la Informació a l'hora d'assegurar un tractament correcte de la informació que gestiona per dur a terme les seues activitats. Els sistemes d'informació i els equips informàtics recolzen totes les funcions de l'Organització i són essencials per a poder desenvolupar els seus processos de negoci.

Política d'utilització del correu electrònic

L'objectiu d'aquest document es establir unes normes, procediments i bones pràctiques respecte d'aquest servei, així com els procediments adients de gestió d'usuaris.

Política d'utilització dels serveis en xarxa

L'objectiu d'aquest document es establir unes normes, procediments i bones pràctiques respecte d'aquest servei, així com els procediments de gestió i accés a aquests recursos.

3.2 Procediment d'Auditories Internes

A l'hora de designar l'equip d'Auditories internes, únicament el personal competent i independent de l'àrea objecte podrà realitzar les auditories.

Tots els membres de l'equip d'Auditories Internes han de ser designats pel Responsable de Seguretat.

Aquest informe serà entregat al Responsable de Seguretat en cas de que aquest no sigui també l'Auditor Cap i aquest serà l'encarregat de mantenir i guardar aquest informe.

3.3 Gestió d'Indicadors

És necessari seleccionar i establir els indicadors adients amb l'objectiu de controlar el funcionament de les mesures de seguretat de la informació implantades a l'Empresa X, d'avaluar l'eficiència i eficàcia de les mateixes i de supervisar l'evolució de l'estat de la Seguretat de la Informació.

Aquests d'indicadors també poden ajudar a mesurar la rendibilitat de les inversions realitzades en matèria de Seguretat en l'Empresa X.

Per tant, s'han de definir els mecanismes i la periodicitat de mesura dels indicadors establerts.

3.4 Procediment de Revisió per Direcció

La Direcció General de l'Empresa X ha de revisar el Sistema de Gestió de la Seguretat de la Informació de l'Organització, com a mínim de manera anual, per tal d'assegurar la seua idoneïtat, adequació i efectivitat.

3.5 Gestió de Rols i Responsabilitats

El Comitè de Direcció de l'Organització és l'encarregat d'avaluar i aprovar les decisions estratègiques quant a la Seguretat de la Informació. Format pels tres membres de la Direcció General de l'empresa, tindrà entre les seues funcions:

3.6 Metodologia d'Anàlisi de Riscos

La metodologia escollida per dur a terme l'anàlisi de riscos en l'Empresa X es fonamenta en els següents procediments:

3.7 Declaració d'Aplicabilitat

A l'arxiu adjunt amb nom "BorregoRodriguezPatricia_SOA 27002_2013_TFM_Fase2.xlsx", es detallen els controls de seguretat de la norma ISO/IEC27002:2013 que s'apliquen o es van a aplicar en l'Organització com a part del desenvolupament i implantació del Sistema de Gestió de Seguretat de la Informació en l'Empresa X.

4. Anàlisi de Riscos

La metodologia que s'ha escollit per dur a terme l'anàlisi de riscos està basada en la metodologia NIST.

Aquesta metodologia és d'origen americà i les valoracions que utilitza es fan des d'un punt de vista qualitatiu.

A l'hora d'analitzar els riscos als que s'exposen els actius de l'empresa, s'ha d'estimar la freqüència i l'impacte que una amenaça pot tenir sobre un actiu o més, aprofitant una vulnerabilitat determinada.

4.1 Inventari d'Actius

Encara que aquest apartat no forma part de les fases establertes en la metodologia NIST, es considera important disposar d'una estimació acurada dels actius a protegir de l'Empresa X.

A l'hora d'identificar i inventariar els actius de l'organització, aquests es poden classificar en cinc tipus possibles:

Actius Hardware: Tots aquells de tipus maquinari emprats en l'empresa, des d'ordinadors a mòbils o impressores.

Actius Programari: Tots els actius software utilitzats, tant propis com de tercers.

Actius Personal: Persones involucrades en el desenvolupament de les activitats de l'empresa, tant treballadors com clients o proveïdors.

Actius Instal·lacions: Tots els elements d'entorn i infraestructura que l'organització necessita perquè la resta funcioni correctament.

Actius Intangibles: Elements importants per a l'empresa però que aquesta no té directament.

Actius Serveis: Tots els serveis que l'empresa proporciona tant de manera interna com externa i que són imprescindibles per a aquesta.

A continuació, es detallen els actius identificats després de dur a terme l'inventari de l'Empresa X.

Aquest inventari consta aproximadament de 65 actius.

ID	*Àmbit*	*Actiu*
1	Instal·lacions	Oficines
2	Personal	Conserges de l'edifici
3	Equipament auxiliar	Càmeres vigilància de l'edifici
4	Equipament auxiliar	Reixa de seguretat extensible porta principal
5	Equipament auxiliar	Claus dels despatxos, porta principal i CPD

6	Equipament auxiliar	Reixes de finestres interiors
7	Instal·lacions	Despatxos Directius
8	Instal·lacions	CPD
9	Equipament auxiliar	Mobiliari oficina: taules, calaixeres, cadires...
10	Equipament auxiliar	Claus de les calaixeres
11	Xarxa	Línia telefònica (inclou telèfons fixos)
12	Xarxa	Línia Internet
13	Hardware	Equips de treball (sobretaula i portàtils)
14	Hardware	Equips i servidors de proves
15	Hardware	Centraleta telefònica
16	Dades	Documentació impresa
17	Instal·lacions	Menjador
18	Instal·lacions	Magatzem
19	Equipament auxiliar	Climatització
20	Equipament auxiliar	SAI
21	Equipament auxiliar	Extintors (oficina i edifici)
22	Equipament auxiliar	Destructora paper
23	Hardware	Impressores i escàner
24	Hardware	2 Servidors Controladors de Domini
25	Hardware	Servidor Repositori de Dades
26	Aplicació	Programari Virtualització VMWare ESX
27	Aplicació	Programari Windows Server 2008 Standard i Windows 7 Professional
28	Serveis	Servei DNS
29	Serveis	Servei DHCP
30	Hardware	Servidor Correu Lotus Notes
31	Hardware	Servidor Correu Web iNotes
32	Aplicació	Programari Lotus Notes (servidors i client)
33	Hardware	Servidor Còpies de seguretat
34	Aplicació	Programari HP Data Protector
35	Hardware	Unitat de cintes externa HP
36	Hardware	Pool de Cintes LTO
37	Hardware	Servidor ERP Producció
38	Serveis	Servei ERP
39	Aplicació	Codi font ERP
40	Aplicació	Programari Base de Dades
41	Hardware	Servidor ERP Proves
42	Hardware	Servidor Base de Dades Producció
43	Hardware	Clúster de servidors físics HP Blade
44	Hardware	Centraleta telefònica
45	Hardware	Router ADSL
46	Hardware	Servidor que executa l'eina Antivirus
47	Aplicació	Programari Antivirus Trend Micro
48	Hardware	Proxy
49	Hardware	Firewall
50	Aplicació	Programari ofimàtic Microsoft Office
51	Personal	Direcció / Directors Departament
52	Personal	Responsable Tècnic
53	Personal	Responsable de Programari
54	Personal	Resta de treballadors
55	Intangible	Know-How Tècnic
56	Intangible	Know-How ERP
57	Intangible	Imatge Corporativa
58	Dades	Informació i documentació corporativa
59	Hardware	Telèfons mòbils
60	Equipament Auxiliar	Cablejat telefònic

61	Equipament Auxiliar	Cablejat xarxa informàtica
62	Equipament Auxiliar	Subministraments essencials (llum, aigua, ...)
63	Serveis	Serveis TIC oferts a clients
64	Serveis	Servei Correu electrònic
65	Hardware	Suports extraïbles (USB, CD, DVD, ...)

4.2 Identificació d'Amenaces

Una amenaça és la probabilitat de que una font particular d'amenaça pugui aprofitar una determinada vulnerabilitat. Una vulnerabilitat és una debilitat que pot ser accidentalment activada o intencionalment explotada. Una amenaça no presenta cap risc si no existeix una vulnerabilitat que pugui ser aprofitada per aquesta.

L'origen d'una amenaça pot ser:

Natural: Amenaces derivades de successos meteorològics i climàtics.

Humà: Amenaces derivades d'una acció intencionada o accidental realitzada per una persona.

Entorn: Amenaces derivades dels elements físics que envolten a l'empresa i la seua informació.

Aquestes amenaces poden afectar a diferents **àmbits de la seguretat de la informació**. En aquesta anàlisi ens centrarem en els tres àmbits principals de la seguretat de la informació:

Confidencialitat: Únicament les persones autoritzades tindran accés a la informació sensible, confidencial i/o privada.

Disponibilitat: La informació estarà disponible per als usuaris autoritzats sempre que sigui necessari.

Integritat: La informació i els seus mètodes de processament són exactes i complets, i no s'han manipulat sense autorització.

Les amenaces identificades i estudiades es troben incloses a l'anàlisi de riscos.

4.3 Identificació de Vulnerabilitats

Una vulnerabilitat és una fallada o debilitat en els procediments de seguretat, disseny, implementació o controls interns d'un sistema que pot ser explotada de manera accidental o intencional, i provocar una bretxa de seguretat o una violació de la política de seguretat del sistema.

La metodologia proposada per NIST considera les vulnerabilitats com a autèntics forats de seguretat, a diferència d'altres metodologies que les entenen com a freqüència d'ocurrència. Per aquest motiu, és pel que

durant l'anàlisi de riscos també s'identifiquen les vulnerabilitats que afecten als actius a protegir.

4.4 Avaluació de Riscos

Després de dur a terme l'inventari d'actius de l'Empresa X que ens permet identificar els actius a protegir, s'ha de realitzar una anàlisi i avaluació dels riscos als que estan exposats aquests actius.

Com que la metodologia escollida per a dur a terme l'anàlisi de riscos està basada en la metodologia NIST, la següent etapa consisteix en identificar les possibles vulnerabilitats que poden afectar a cadascun dels actius i les amenaces que poden aprofitar aquestes vulnerabilitats.

Altres factors a tenir en compte en aquesta anàlisi són l'origen de l'amenaça i les característiques o àmbits de la seguretat de la informació que quedarien afectades si s'arribés a materialitzar aquesta.

Una vegada reunida tota la informació d'interès dels diferents escenaris avaluats, s'ha d'estimar la probabilitat de que aquesta situació s'arribi a donar, així com l'impacte que podria provocar en l'empresa. Prenent com a base l'encreuament d'aquesta probabilitat i aquest impacte, es determina el risc a què està exposada l'organització.

Per dur a terme aquesta estimació s'utilitzarà la taula definida a l'apartat 3.6. Metodologia d'Anàlisi de Riscos.

Probabilitat d'amenaça	***Impacte***		
	Baix	**Mitjà**	**Alt**
Baix	Baix	Baix	Baix
Mitjà	Baix	Mitjà	Mitjà
Alt	Baix	Mitjà	Alt

Sospesant els diferents escenaris que poden afectar als actius de l'empresa, aconseguirem identificar els riscos als que està exposada l'Empresa X, per tal de classificar-los, mesurar-los i prioritzar el seu tractament adientment.

A l'arxiu Excel adjunt amb nom "BorregoRodriguezPatricia_Avaluació Riscos_Fase3.xlsx", en la pestanya d'Avaluació de Riscos, es detalla l'avaluació de riscos realitzada.

4.5 Nivell de Risc Acceptable

Una vegada realitzada l'anàlisi de riscos i identificats els riscos que suposen un major perill per als actius de l'Empresa X, aquesta informació es porta front al Comitè de Direcció que és l'organisme que ha d'avaluar i decidir el nivell de risc que l'organització pot assumir.

D'un total de 75 riscos avaluats, 17 d'aquests es cataloguen com a risc alt; 35 són riscos amb un nivell mitjà i 23 estan catalogats com a risc baix.

Com que l'empresa es troba al començament de la implantació del SGSI, i compta amb un pressupost limitat, la Direcció decideix establir el nivell de risc acceptable en un nivell mitjà, assumint les conseqüències dels riscos de nivells igual o inferior a aquest.

La decisió de la Direcció en aquesta primera etapa d'implantació del SGSI, és centrar els seus esforços i recursos en reduir els riscos amb un nivell alt, i en posteriors avaluacions de riscos, anar reduint el nivell de risc acceptable per l'organització.

Per tant, es proposaran i implantaran mesures de control per als 17 riscos catalogats com alts, que en la situació actual són els que poden posar en perill els processos de negoci, evitant que aquests es duguin a terme adientment amb una major probabilitat.

4.6 Determinació del Risc Residual

Una vegada s'hagin escollit els controls adients a aplicar sobre els 17 riscos a tractar, es tornarà a avaluar el nivell de risc després de l'aplicació de les mesures de seguretat, és a dir, es calcularà el nivell de risc residual.

Tractament dels riscos

Per a cadascun dels riscos a tractar després d'avaluar l'anàlisi de riscos és necessari prendre un decisió quant al tractament d'aquest. Les opcions possibles inclouen:

- Aplicació de controls adients per a reduir el risc.
- Acceptar el risc conscient i objectivament.
- Evitar el risc prohibint les accions que podrien causar que el risc es produeixi.
- Transferir el risc associat a altres grups, com asseguradores o proveïdors.

Com s'ha explicat en l'apartat anterior, la Direcció ha decidit acceptar els riscos amb un nivell mitjà o inferior.

A l'arxiu Excel adjunt amb nom "BorregoRodriguezPatricia_Avaluació Riscos_Fase3.xlsx", en la pestanya de Riscos Residuals, es detalla el càlcul del risc residual per als 17 riscos amb nivell alt, després de l'aplicació del control de seguretat adequat.

Després d'aplicar el control de seguretat adient, el nivell de risc residual per als 17 riscos tractats queda per baix del nivell de risc acceptable.

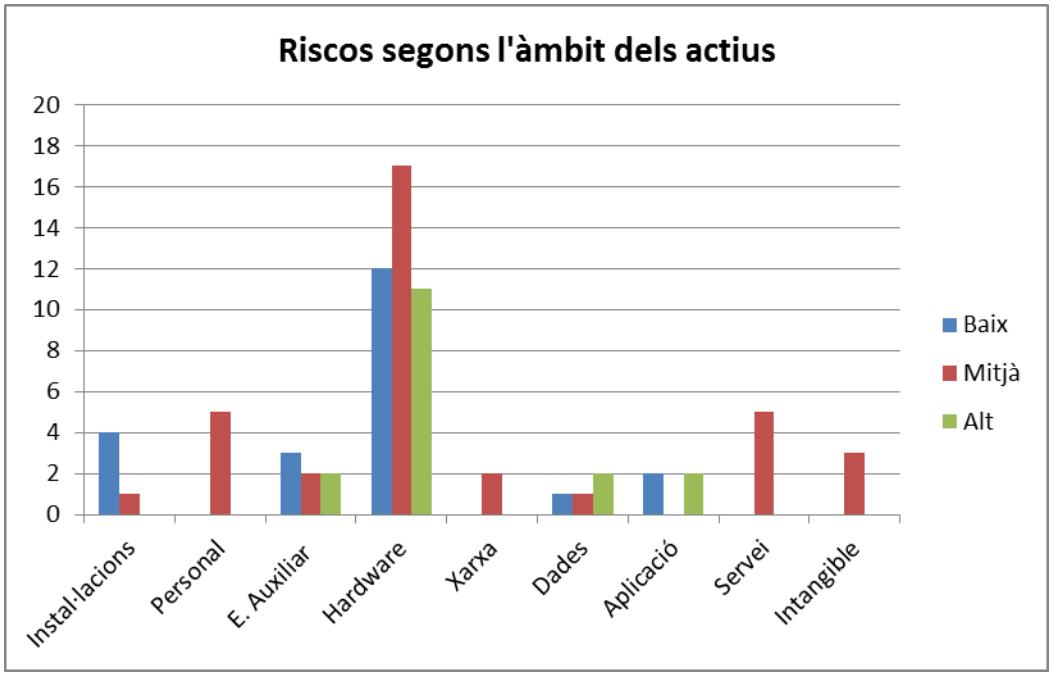
En posteriors cicles d'aplicació del SGSI i després de dur a terme noves anàlisis de riscos, es determinarà un nou nivell de risc acceptable i el nivell de cadascun dels riscos detectats per a tractar-los segons sigui necessari.

4.7 Conclusió

Una vegada realitzada l'anàlisi de riscos podem valorar la situació de l'Empresa X quant als tipus de riscos que poden posar en perill els actius d'informació de l'organització amb més probabilitat i decidir quins dels riscos contemplats en aquesta anàlisi es tractaran mitjançant les propostes incloses al Pla de Projectes.

Per a prendre aquesta decisió, ens ajudarem de diferents gràfics que ens permetran tenir una visió globalitzadora de la situació de l'empresa i de les condicions a tenir en compte a l'hora de continuar amb la següent fase del SGSI.

En primer lloc, mostrem un gràfic en el que es pot avaluar la quantitat i nivell de criticitat dels riscos que afecten a cada tipus o àmbit d'actiu.

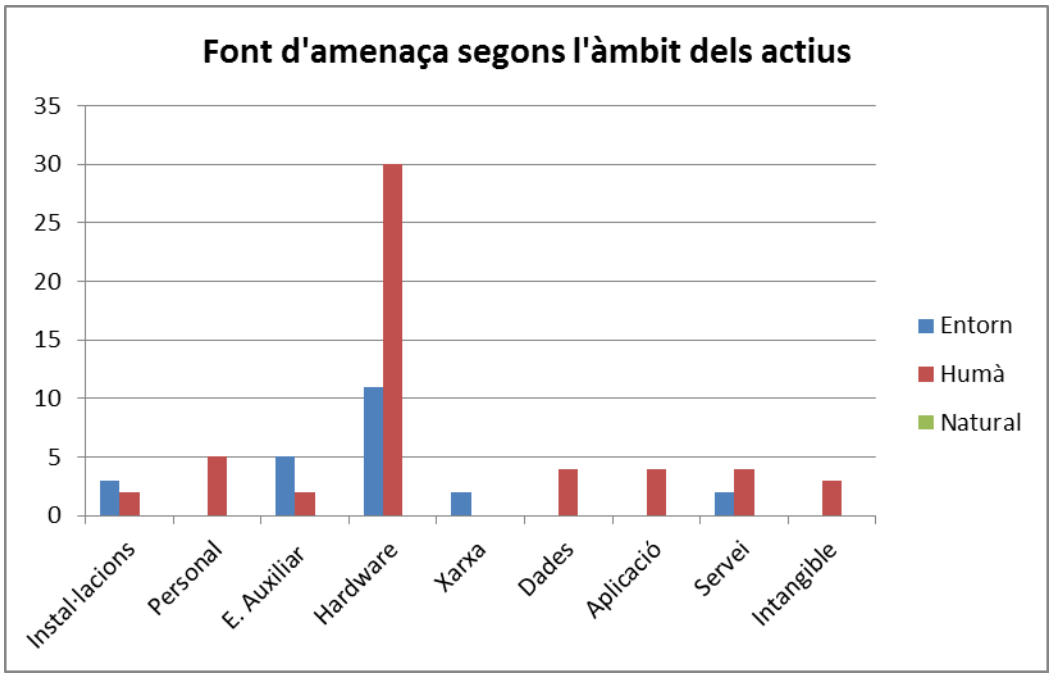


Com és d'esperar, els *àmbits d'actiu més vulnerables* de l'Empresa X, pel tipus de sector en el que treballa i pel tipus de serveis que proveeix, són l'àmbit **Hardware**, seguit de l'àmbit de **Serveis** i del de **Personal**.

Aquests àmbits són els que més riscos presenten junt amb l'àmbit d'Instal·lacions. La diferència amb aquest últim és que de 5 riscos que presenta, 4 són de nivell baix.

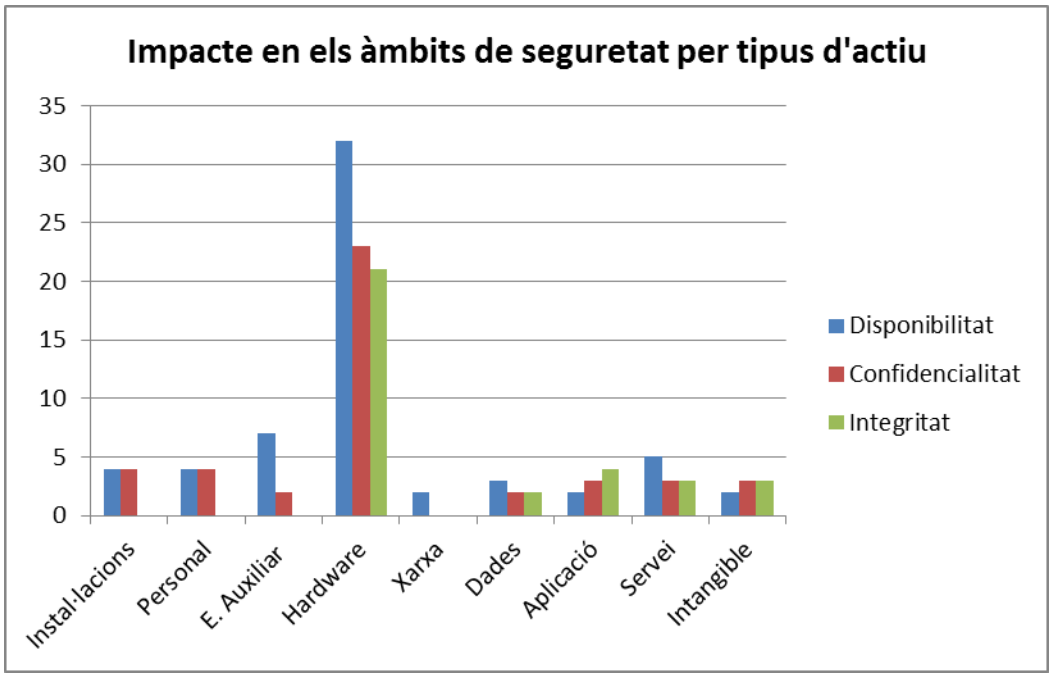
Queda comprovat que el correcte funcionament tant com els processos de negoci de l'organització depenen fonamentalment d'aquests tres tipus d'actius.

En segon lloc, s'avaluen les fonts d'amenaça més freqüents per cadascun dels àmbits dels actius, que poden afectar a l'Empresa X.



Després d'analitzar la gràfica anterior queda clar que la *font més comuna d'amenaça* en quasi tots els àmbits és la **humana**.

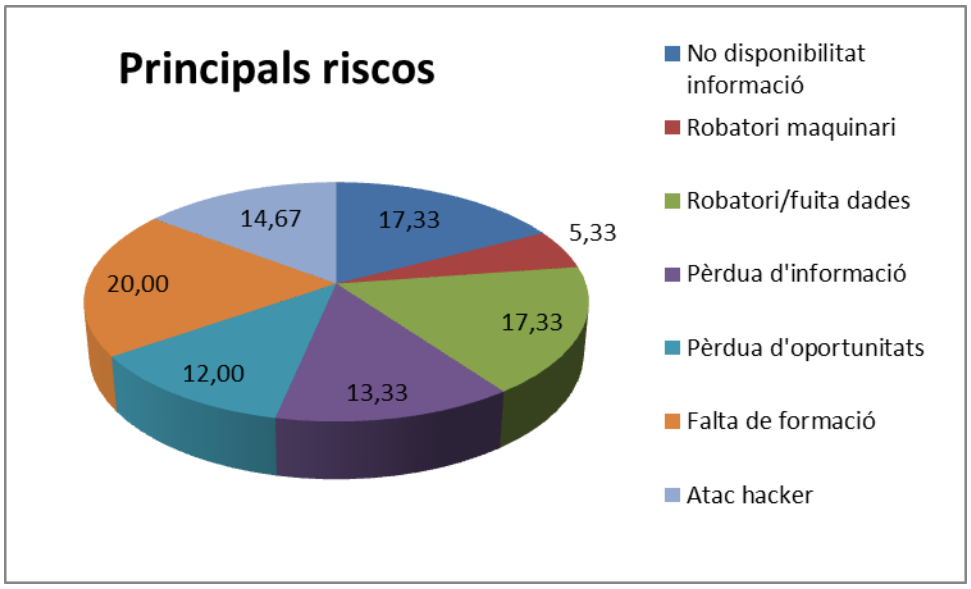
Quan estudiem els impactes que poden provocar les vulnerabilitats i amenaces analitzades a nivell d'àmbits de seguretat i classificant aquests impactes pel tipus o àmbit d'actiu, trobem els següents resultats:



Com era d'esperar, els actius de tipus hardware continuen sent els més vulnerables en qualsevol dels *àmbits de seguretat* estudiats a l'anàlisi de riscos. Però a nivell global, trobem que l'àmbit de seguretat que sofreix un major impacte és el de la **disponibilitat** dels actius.

A l'hora de determinar els *principals riscos* que poden afectar a l'Empresa X, hem de tenir en compte que la metodologia escollida per dur a terme l'anàlisi de riscos no parla de riscos concrets, si no que a partir de la combinació d'una vulnerabilitat i una amenaça concretes, es determina l'impacte del risc que suposa aquesta combinació.

Per aquest motiu, i amb la finalitat d'extreure un llistat dels principals riscos a tractar en la següent fase, es partirà d'aquestes combinacions de parells vulnerabilitat-amenaça i es classificaran dins una selecció de riscos més generals. Serà aquest llistat de riscos el que es representi gràficament.



De la classificació general dels riscos proposada, els *principals riscos* que afecten o poden afectar a l'organització són la **falta de formació**, la **no disponibilitat d'informació** durant un temps prolongat o el **robatori o fuita de les dades o informació** de l'empresa.

En conclusió, en la següent fase, a l'hora de proposar projectes a implantar per millorar el nivell de seguretat de la informació de l'Empresa X, l'objectiu principal d'aquests serà reduir la probabilitat de materialització dels principals riscos detectats: falta de formació, no disponibilitat d'informació i el robatori o fuita d'informació.

Els projectes estaran orientats a:

- protegir els àmbits més vulnerables de l'Empresa X: Hardware, Serveis i Personal.
- conscienciar i formar en matèria de seguretat de la informació, a la font més comuna d'amenaces, que és la humana.
- reduir l'impacte de les amenaces sobre la disponibilitat dels actius d'informació.

5. Propostes de Projectes

A partir dels resultats obtinguts en la fase d'anàlisi de riscos, es proposen projectes dirigits a millorar la gestió de la seguretat de la informació així com la optimització dels recursos i la gestió de processos i tecnologies utilitzades en l'Empresa X.

A continuació es detallen i descriuen els diferents projectes proposats.

5.1 Contractació d'una línia de connexió a Internet de backup

Taula Resum

Definició	**La disponibilitat d'Internet en una empresa com l'Empresa X és un element fonamental i necessari per poder dur a terme els processos de negoci d'aquesta. La instal·lació de una línia d'Internet de backup proporciona la redundància necessària per assegurar la disponibilitat d'aquesta eina de treball.**
Objectius	Evitar la no disponibilitat de connexió a Internet durant un període de temps prolongat i proporcionar redundància de servei.
Beneficis	Disponibilitat del servei per poder realitzar les tasques diàries que conformen els processos de negoci i evitar pèrdues d'oportunitats com a conseqüència de la falta de connexió a Internet.
Riscos a mitigar	Riscos concrets: ID12 - ID13 Principals riscos: Atac hacker - Pèrdua d'oportunitats
Controls ISO relacionats	11.2.2 - 17.2

Desenvolupament

La utilització d'Internet per dur a terme els processos de negoci a l'Empresa X és fonamental ja que és necessari per realitzar una gran quantitat de tasques diàries de les que depèn la continuïtat i èxit de l'organització.

No disposar d'aquest servei durant un temps prolongat pot causar pèrdua d'oportunitats, no disponibilitat d'informació necessària per dur a terme les tasques diàries de l'empresa, i en general, la disminució en la qualitat dels serveis oferts als seus clients.

Per aquest motiu, es proposa contractar una segona línia de connexió a Internet amb l'objectiu de redundar un dels serveis bàsics que els treballadors de l'organització utilitzen ja com una eina més en el desenvolupament del seu treball diari.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació del Responsable Tècnic, el Director d'Infraestructures i el Comitè de Direcció, a nivell intern. A més, serà necessària la participació del tècnic d'instal·lació del mòdem de la companyia contractada.

El Responsable Tècnic s'encarregarà de determinar el tipus de connexió més adient a contractar, demanar pressupost a diferents companyies i decidir la companyia amb la que es contractarà el servei de connexió a Internet de backup.

El Director d'Infraestructures supervisarà el projecte, la contractació del servei i pressupost derivat de la implantació del projecte.

El Comitè de Direcció avaluarà la idoneïtat del projecte i el dotarà dels recursos necessaris per la seua implantació.

El tècnic de la companyia realitzarà la instal·lació i configuració corresponent de la línia de connexió i el mòdem/router corresponent.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat completament en un termini de dos setmanes.

Quantificació econòmica

- Contractació del servei + instal·lació/configuració: 135€
- Quota mensual per un any: 40€ * 12 mesos = 480€
- Hores Responsable Tècnic (50h aproximadament a 20€/h): 1000€
- Hores Director Infraestructures (1.5h aprox. a 40€/h): 60€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 1855€

5.2 Millora de la seguretat física de l'empresa

Taula Resum

Definició	**Un dels principals riscos detectats durant l'anàlisi de riscos és el robatori o fuita d'informació. Una de les causes principals d'aquest risc és que actualment les mesures de seguretat a nivell físic implantades en l'Empresa X són poques i gaire febles.**
Objectius	Millorar el nivell de seguretat física de l'organització mitjançant la implantació d'un sistema de vigilància propi i adaptat a les necessitats concretes de l'empresa. Reforçament de les mesures de seguretat físiques implantades a l'edifici d'oficines.
Beneficis	Evitar accessos no autoritzats a les instal·lacions. Detecció immediata d'intents no autoritzats d'accés. Reducció de riscos de robatori o traspàs.
Riscos a mitigar	Riscos concrets: ID3 - ID4 - ID5 - ID6 - ID7 - ID16 - ID18 - ID20 - ID50 Principals riscos: Robatori maquinari - Robatori/fuita dades - No disponibilitat informació
Controls ISO	11.1.1

relacionats

Desenvolupament

Un dels principals riscos detectats durant l'anàlisi de riscos és el robatori o fuita d'informació. Una de les causes principals d'aquest risc és que actualment les mesures de seguretat a nivell físic implantades en l'Empresa X són poques i gaire febles, ja que la majoria depenen de la seguretat implantada en l'edifici en el que se situen les oficines de l'organització.

El problema és que aquestes mesures implantades a nivell de l'edifici no depenen de l'empresa i per tant, no poden saber si estan implantades adientment o si funcionen correctament.

Per aquest motiu, es proposa implantar mesures de seguretat física a nivell de les pròpies oficines de l'empresa i deixar de dependre completament de les mesures implantades a l'edifici per aconseguir un nivell de seguretat adient.

Dins aquest projecte es contempla la contractació d'un servei d'alarma i amb sensors de detecció de moviment connectats a la central del servei d'alarma.

Amb la implantació d'aquest projecte es reduiran considerablement totes les possibles amenaces i riscos associats a l'accés físic no autoritzat a les oficines i el robatori físic de dades i informació corporativa.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació del empleat del Departament d'Administració, del Director d'Administració i del Comitè de Direcció, a nivell intern. A més, serà necessària la participació del tècnic d'instal·lació del servei d'alarma amb els sensors de detecció de moviment de la companyia contractada.

L'empleat del Departament d'Administració s'encarregarà de cercar informació sobre el tipus de servei de vigilància més adient a contractar i demanar pressuposts a diferents companyies.

El Director d'Administració decidirà la companyia amb la que es contractarà el servei, a més de negociar el pressupost final. Al tractar-se d'un projecte que afecta a les instal·lacions de l'empresa i a la forma d'accedir a aquesta de tots els treballadors, el Director portarà la proposta al Comitè de Direcció per obtenir l'aprovació i suport econòmic d'aquest.

El Comitè de Direcció avaluarà la idoneïtat del projecte i el dotarà dels recursos necessaris per la seua implantació.

Una vegada aprovat el projecte per la Direcció de l'Empresa X, el tècnic de la companyia realitzarà la instal·lació i configuració corresponent al servei d'alarma, dels sensors de detecció de moviment i de qualsevol altre equipament inclòs en el servei.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, és a dir, des que es comença a cercar informació de companyies que ofereixen aquest servei fins que l'alarma i els sensors estan instal·lades i funcionant correctament, pot estar implantat completament en un termini de tres setmanes.

Quantificació econòmica

- Contractació del servei + instal·lació/configuració: 210€
- Quota mensual per un any: 50€ * 12 mesos = 600€
- Hores Empleat Administració (50h aprox. a 12€/h): 600€
- Hores Director Administració (8h aprox. a 40€/h): 320€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 1910€

5.3 Control d'accés digital al CPD

Taula Resum

Definició	**Un dels principals riscos detectats durant l'anàlisi de riscos és el robatori o fuita d'informació. El CPD de l'empresa és la sala on es troben la informació i els sistemes més crítics de l'organització. Per tant és necessari protegir-ho adientment.**
Objectius	Millorar el control d'accés al CPD de l'organització mitjançant la implantació d'un sistema d'accés amb petjada digital. Monitorització i supervisió dels accessos autoritzats i intents d'accessos no autoritzats. Definició i configuració de permisos d'accés del personal. Reforçament de les mesures de seguretat físiques implantades a l'edifici d'oficines.
Beneficis	Evitar accessos no autoritzats al CPD. Detecció immediata d'intents no autoritzats d'accés. Protecció de sistemes i informació crítiques. Reducció de riscos de robatori o traspàs.
Riscos a mitigar	Riscos concrets: ID3 - ID4 - ID5 - ID6 - ID7 - ID18 - ID20 - ID50 Principals riscos: Robatori maquinari - Robatori/fuita dades - No disponibilitat informació
Controls ISO relacionats	9.1 - 9.2 - 11

Desenvolupament

Després de dur a terme l'anàlisi de riscos queda clar que els actius de tipus hardware i la informació que aquests emmagatzemen són uns dels actius més importants de l'empresa.

Sense un correcte funcionament dels servidors ubicats en el CPD o mitjançant el robatori o trencament d'aquestes màquines i de la informació continguda, es podria aconseguir un impacte molt greu i crític sobre els negocis de l'organització.

Per aquest motiu, es proposa la implantació d'un control d'accés amb petjada digital per accedir al CPD de l'Empresa X i a totes les màquines ubicades en aquesta sala.

Mitjançant aquest tipus de control es podria monitorar qualsevol accés al CPD, tant en horari laboral com fora d'aquest i es garantiria que únicament les persones amb autorització per accedir-hi, podrien entrar al CPD.

A més, amb la implantació d'aquest projecte aconseguiríem reduir els riscos de robatori d'informació o no disponibilitat, derivats d'actes de vandalisme o d'accessos físics no autoritzats que podrien causar danys en les màquines físiques allotjades al CPD.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació del Responsable Tècnic, del Director d'Infraestructures i del Comitè de Direcció, a nivell intern. A més, serà necessària la participació del tècnic d'instal·lació del servei de control d'accés de la companyia contractada i de la mà d'obra necessària per canviar la porta d'accés al CPD per una connectada al panel de control de petjada digital.

El Responsable Tècnic s'encarregarà de determinar el tipus de servei de control d'accés al CPD més adient a contractar, demanar pressuposts a diferents companyies i decidir la companyia amb la que es contractarà el servei, a més de negociar el pressupost.

El Director d'Infraestructures supervisarà la contractació del servei i pressupost derivat. El Director també s'encarregarà de portar la proposta al Comitè de Direcció per obtenir l'aprovació i suport econòmic d'aquest.

El Comitè de Direcció avaluarà la idoneïtat del projecte i el dotarà dels recursos necessaris per la seua implantació.

Una vegada aprovat el projecte per la Direcció de l'Empresa X, en primer lloc es canviarà la porta d'accés al CDP per una que es pugui connectar al panel de control a instal·lar i a continuació, el tècnic de la companyia realitzarà la instal·lació i configuració del panel de control d'accés, a més d'explicar al Responsable Tècnic el funcionament del programari de gestió de petjades digitals.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat completament en un termini de tres setmanes.

Quantificació econòmica

- Canvi de porta d'accés al CPD + Porta nova: 600€
- Contractació del servei + instal·lació/configuració del panel + programari de gestió de petjades digitals: 800€
- Hores Responsable Tècnic (72h aproximadament a 20€/h): 1440€
- Hores Director Infraestructures (2h aprox. a 40€/h): 80€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 3100€

5.4 Condicionament del CPD

Taula Resum

Definició	**Si les condicions ambientals no són les adequades dins el CPD de l'empresa, això pot tenir com a conseqüència directa la no disponibilitat de la informació i els serveis que les màquines allotjades al CPD proporcionen. Per evitar aquesta situació, es necessari aplicar les mesures de condicionament adients.**
Objectius	Evitar la no disponibilitat dels serveis allotjats al CDP per amenaces d'origen ambiental, com pot ser calor excessiu o pèrdua d'alimentació. Prevenir el mal funcionament o fallada de màquines o serveis causats per motius ambientals.
Beneficis	Disponibilitat de la informació i els serveis necessaris per poder realitzar les tasques diàries que conformen els processos de negoci i evitar pèrdues d'oportunitats o d'informació com a conseqüència de la fallada de les màquines. Rendiment òptim de les màquines i dispositius. Assegurar un apagat controlat de les màquines del CPD. Evitar un calfament excessiu de les màquines en els mesos de calor.
Riscos a mitigar	Riscos concrets: ID8 - ID14 - ID15 Principals riscos: No disponibilitat informació - Pèrdua d'oportunitats
Controls ISO relacionats	11

Desenvolupament

Un dels principals riscos que poden afectar a l'Empresa X és la no disponibilitat de la informació emmagatzemada en els servidors del CPD que pot materialitzar-se amb una probabilitat prou alta quan es produeixen una d'aquestes dues situacions:

- Un calor excessiu dins el CPD per falta de potència del servei d'aire condicionat centralitzat de les oficines i accentuat als mesos de calor per la situació geogràfica de les oficines de l'organització.
- Un tall prolongat del subministrament elèctric per falta d'autonomia del SAI actual.

Si qualsevol d'aquestes situacions es produeix per un temps prolongat és molt probable que les màquines comencen a fallar i com a conseqüència directa, la informació no estigui disponible per als treballadors.

Per aquest motiu, es proposa la instal·lació d'un aparat d'aire condicionat per al CPD, exclusiu i independent del de la resta de les oficines, ja que l'aire condicionat general no té potència suficient per mantenir una temperatura ambiental adequada en el CPD.

A més, també com a part d'aquest projecte es proposa canviar el SAI que actualment està instal·lat al CPD per altre amb més capacitat d'autonomia en les bateries, ja que l'actual no té capacitat suficient per permetre fer un apagat controlat de totes les màquines quan es produeix un tall prolongat al subministrament elèctric i com a conseqüència algunes màquines poden fer un apagat no controlat i produir-se un dany en el sistema operatiu o les dades que conté la màquina en qüestió.

Introduint aquests dos elements com a millora de les condicions actuals del CPD es podrien reduir en un percentatge molt elevat tots els riscos de no disponibilitat de la informació relacionats amb amenaces amb una font de tipus entorn.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació del Responsable Tècnic, del Director d'Infraestructures, d'un empleat d'Administració, del Director d'Administració i del Comitè de Direcció, a nivell intern. A més, serà necessària la participació del tècnic d'instal·lació de l'aparat d'aire condicionat i del tècnic d'instal·lació i configuració del SAI.

El Responsable Tècnic s'encarregarà de determinar el tipus de SAI a instal·lar més adient, demanar pressuposts a diferents companyies i decidir la companyia amb la que es contractarà el servei, a més de negociar el pressupost final.

El Director d'Infraestructures supervisarà la contractació del servei i pressupost derivat. El Director també s'encarregarà de portar la proposta al Comitè de Direcció per obtenir l'aprovació i suport econòmic d'aquest.

L'empleat del Departament d'Administració s'encarregarà de cercar informació sobre els aparats d'aire condicionat a instal·lar i demanar pressuposts a diferents companyies.

El Director d'Administració decidirà la companyia amb la que es contractarà el servei, a més de negociar el pressupost final. El Director també s'encarregarà de portar la proposta al Comitè de Direcció per obtenir l'aprovació i suport econòmic d'aquest.

El Comitè de Direcció avaluarà la idoneïtat dels dos serveis que conformen el projecte i el dotarà dels recursos necessaris per la seua instal·lació.

Una vegada aprovat el projecte per la Direcció de l'Empresa X, en primer lloc es canviarà i configurarà el SAI del CDP i a continuació, es realitzarà la instal·lació de l'aparat d'aire condicionat.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat completament en un termini de mes i mig.

Quantificació econòmica

- Contractació del servei+ + instal·lació/configuració del SAI i les bateries: 2964€
- Contractació del servei + instal·lació de l'aire condicionat: 815€
- Hores Responsable Tècnic (65h aprox. a 20€/h): 1300€
- Hores Director Infraestructures (2.5h aprox. a 40€/h): 100€
- Hores Empleat Administració (48h aprox. a 12€/h): 576€
- Hores Director Administració (8h aprox. a 40€/h): 320€
- Hores Comitè Direcció (2h a 60€/h * 3 membres): 360€

Pressupost total: 6435€

5.5 Desenvolupament d'un Pla de Continuïtat

Taula Resum

Definició	**La continuïtat del negoci és un aspecte fonamental i crític per l'Empresa X. Per aquest motiu, és necessari desenvolupar un Pla de Continuïtat que estableixi els procediments a seguir en cas de desastre.**
Objectius	Evitar la no disponibilitat dels processos crítics de l'organització o aconseguir reduir al màxim el temps de no disponibilitat d'aquests.
Beneficis	Establir els procediments a executar en cas de necessitat. Anticipació al desastre. Assegurament de la continuïtat del negoci.
Riscos a mitigar	Riscos concrets: Qualsevol risc que excedeixi les mesures de seguretat implantades i el seu abast posant en risc els processos de negoci de l'Empresa X. Principals riscos: Pèrdua d'informació - No disponibilitat informació - Robatori maquinari - Robatori/fuita dades - Pèrdua d'oportunitats - Falta de formació - Atac hacker

Controls ISO relacionats	6.1.3 - 12.2.1 - 12.3.1. - 17.1

Desenvolupament

Un element fonamental a l'hora d'assegurar i preservar els processos de negoci crítics de l'Empresa X 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 va un pas més enllà a l'hora d'evitar les interrupcions en l'activitat de negoci i intenta minimitzar el temps d'inactivitat si es produeixen aquestes interrupcions.

Com a proposta de Pla de Continuïtat es proposa contractar un lloguer d'instal·lacions que servirà per guardar les cintes LTO amb còpies setmanals i xifrades fora de les oficines de l'empresa així com per a emmagatzemar l'actual entorn virtual format per dos servidors físics i el calaix de discos compartits actual.

Aquest entorn virtual passarà a ser l'entorn de backup del nou entorn (proposta 5.10) i que s'utilitzarà per a tenir el sistema de màquines virtuals i de dades de l'empresa replicat i a punt per a substituir de manera temporal al nou, en cas d'emergència. La informació continguda podrà tenir fins a dues setmanes d'antiguitat i segons el tipus d'emergència podria ser necessari comprar equips de treball de substitució o que els treballadors utilitzen de forma temporal els seus equips personal.

Com a part d'aquest Pla, també s'inclouen les hores de manteniment i actualització que uns determinats treballadors del Departament d'Infraestructures hauran d'invertir cada 15 dies en mantenir a punt aquest sistema de respatller.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, de:

- 3 treballadors del Departament d'Infraestructures
- Responsable Tècnic i Responsable de Programari
- Responsable de Seguretat
- 3 Directors departamentals
- Comitè de Direcció

Els Responsables Tècnic, de Programari i de Seguretat, seran els encarregats de definir el Pla de Continuïtat, els procediments de integrants d'aquest.

A continuació, es durà a terme una reunió entre els Director d'Infraestructures, el Director Comercial, el Director d'Administració i el Responsable de Seguretat, on s'exposarà el pla proposat i com afecta a cadascun dels departaments de l'empresa. Es valorarà la seua viabilitat amb la intervenció o no, segons escaigui, de personal d'altres departaments.

Per últim, el Responsable de Seguretat presentarà la proposta de Pla de Contingència davant el Comitè de Direcció, el qual avaluarà la idoneïtat del Pla i el dotarà dels recursos necessaris per la seua implantació.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps mig. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini de sis mesos.

En qualsevol cas, aquest Pla serà una acció continua i per tant, anirà actualitzant-se i evolucionant segons les necessitats de l'Empresa X.

Quantificació econòmica

- Hores Responsable Tècnic (150h aprox. a 20€/h): 3000€
- Hores Responsable Programari (150h aprox. a 20€/h): 3000€
- Hores Responsable Seguretat (200h aprox. a 30€/h): 6000€
- Hores 3 Directors departamentals (5h aprox. a 40€/h): 600€
- Hores Comitè Direcció(2h a 60€/h * 3 membres): 360€
- Contractació de servei de lloguer d'emmagatzematge extern d'un any amb connexió Internet i altres serveis inclosos:4000€
- Hores 3 Treballadors, 2 tècnics i 1 programador (5h cada 2 setmanes a 12€ durant un any): 4688€

Pressupost total: 21648€

5.6 Desenvolupament d'un Pla de Formació Continua en Seguretat de la Informació

Taula Resum

Definició	**La falta de formació en matèria de seguretat és altre dels principals riscos detectats mitjançant l'anàlisi realitzat. També és una de les principals causes de les que poden derivar multitud d'incidents. Invertir en la formació dels treballadors és invertir en millorar la seguretat dels actius de l'empresa.**
Objectius	Formar i conscienciar als treballadors en matèria de seguretat de la informació segons les seues responsabilitats i tasques a desenvolupar en el seu treball diari.
Beneficis	Millora en el tractament de la informació. Gestió dels actius complint els requeriments legals vigents. Incorporació de bones pràctiques de seguretat en el desenvolupament de les tasques a realitzar i per tant en els processos de negoci.

Riscos a mitigar	Riscos concrets: ID19 - ID28 - ID32 - ID33 - ID40 - ID43 - ID53 - ID56 - ID59 - ID61- ID62 - ID64 - ID67 - ID68 - ID71 - ID72 - ID75 Principals riscos: Falta de formació - Atac hacker
Controls ISO relacionats	5.1.1 - 7.2.2 - 16.1.6

Desenvolupament

Altre dels principals riscos detectats que poden afectar greument a l'Empresa X és la falta de formació en seguretat de la informació dels seus empleats. Aquesta falta de coneixements en bones pràctiques i mesures de seguretat a aplicar en el seu treball diari pot ser l'origen d'una gran quantitat de riscos que tenen com punt feble als treballadors de l'empresa.

Per aquest motiu i amb la intenció de consolidar la formació en seguretat com una tasca continua i necessària per a tots els treballadors, es proposa desenvolupar un Pla de Formació en Seguretat de la Informació.

En aquest pla s'impartirà formació fonamental quant a conscienciació i bones pràctiques a aplicar en el lloc de treball, entre d'altres:

- Contrasenyes robustes i ús de gestors de contrasenyes
- Política de taules netes
- Classificació d'informació i el seu etiquetatge
- Xifrat d'informació a transmetre i en dispositius mòbils i extraïbles
- Procediments de notificació a utilitzar si es detecta un incident de seguretat
- Pautes a aplicar per evitar possibles atacs de phishing i enginyeria social
- Destrucció segura d'informació
- Reutilització de suports extraïbles, esborrat segur

A banda, també s'impartirà formació sobre aspectes i requeriments legals com:

- LOPD i RDLPOD: Classificació i tractament d'informació personal
- LPI: Pagament de taxes per utilització de llicències de programari i similars

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, del Responsable de Seguretat i el Comitè de Direcció.

El Responsable de Seguretat s'encarregarà de fer una proposta de Pla de Formació i de cercar informació sobre companyies que puguin impartir aquesta.

Una vegada seleccionada l'empresa que s'encarregarà de dur a terme les jornades de formació i conscienciació, es negociarà com seran les sessions formatives, el material que l'empresa de formació generarà com a part de les sessions, el material que l'Empresa X haurà de proporcionar per poder realitzar les sessions i la informació a transmetre amb aquestes.
A més, el Responsable de Seguretat s'encarregarà de supervisar la generació de material i el desenvolupament del Pla de Formació així com de realitzar propostes d'actualització i millora.

El Comitè de Direcció avaluarà la idoneïtat del projecte i una vegada aprovat, el dotarà dels recursos necessaris per a la seua realització.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps llarg. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini d'un any.

En qualsevol cas, aquest Pla serà una acció continua i per tant, anirà actualitzant-se i evolucionant segons les necessitats de l'Empresa X i es realitzaran accions formatives amb diversos formats tots els anys.

Quantificació econòmica

- Contractació del servei amb l'empresa de Formació: 23000€
- Hores Responsable Seguretat (300h aprox. a 30€/h): 9000€
- Hores Comitè Direcció(2h a 60€/h * 3 membres): 360€
- Despeses de compres de material addicional: 2000€

Pressupost total: 34360€

5.7 Desenvolupament d'una Política de Classificació i Etiquetat de la Informació

Taula Resum

Definició	**La informació ha de ser tractada i gestionada segons la seua criticitat. Una forma de definir i fonamentar aquesta criticitat és desenvolupar una Política de Classificació d'aquesta informació i així establir com tractar la informació adientment.**
Objectius	Classificar i etiquetar correctament tota la informació generada i manipulada per l'Empresa X, aplicant les mesures de seguretat que corresponguin segons aquesta classificació.
Beneficis	Establiment dels nivells de criticitat de la informació. Definició de les mesures de seguretat corresponents a cada nivell. Compliment amb la legislació vigent. Protecció adequada de la informació manipulada per l'empresa.
Riscos a mitigar	Riscos concrets: ID17 - ID18 - ID26 - ID35 - ID41 - ID69 - ID74 Principals riscos: Robatori/fuita de dades - Atac hacker
Controls ISO relacionats	5.1.1 - 7.1 - 8 - 9.1.1 - 11.2.9 - 15.1.2 - 18.1.3

Desenvolupament

A l'hora d'implantar mesures de seguretat efectives en la protecció de les dades que emmagatzema i tracta l'Empresa X és necessari desenvolupar una Política de Classificació d'Informació amb la que poder determinar el nivell de criticitat i importància d'una determinada informació i saber, en conseqüència, la manera adequada de tractar-ho.

Per aquest motiu, es proposa el desenvolupament d'una Política de Classificació d'Informació i a partir d'aquesta, el desenvolupament dels procediments adients a l'hora de tractar cadascun dels nivells de criticitat de la informació i d'etiquetatge dels suports que emmagatzemen aquesta.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, del Responsable de Seguretat, del Director d'Infraestructures, el Director d'Administració i de Comercial, i el Comitè de Direcció.

El Responsable de Seguretat, junt amb els tres Directors departamentals, seran els responsables de desenvolupar la Política de Classificació d'Informació, on s'establiran els diferents nivell d'informació que es tracte en l'empresa i el procediment per a classificar aquesta adientment. Sempre tenint en compte i basant-se en els requeriments a nivell legal que l'empresa està obligada a complir en el tractament dels diferents tipus d'informació que emmagatzemen i tracten per a dur a terme els seus processos de negoci.

Una vegada la política de classificació està consensuada i aprovada, serà el torn d'establir els procediments d'etiquetatge de la informació, basats en la política de classificació, tant quan la informació està en format electrònic com quan està en format paper.

El Comitè de Direcció avaluarà la idoneïtat del projecte i després de donar el vist i plau, el dotarà dels recursos necessaris per a la seua implantació.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps mig. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini de quatre mesos.

En qualsevol cas, aquesta Política de Classificació i Etiquetatge d'Informació serà tractada com una acció continua i per tant, anirà actualitzant-se i evolucionant segons les necessitats de l'Empresa X.

Quantificació econòmica

- Pressupost estimat per a despeses derivats de la política: 2000€
- Hores Responsable Seguretat (240h aprox. a 30€/h): 7200€
- Hores 3 Directors departamentals (80h aprox. a 40€/h): 9600€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 18980€

5.8 Desenvolupament d'una Política de xifrat de dades.

Taula Resum

Definició	**Quan es tracta i manipula informació sensible i confidencial s'ha de fer amb les mesures de seguretat necessàries. Sobre tot quan aquesta informació s'ha d'enviar a tercers o eix de les instal·lacions de l'empresa.**
Objectius	Protegir la informació corporativa adientment.
Beneficis	Compliment de la legislació vigent. Protecció de la informació confidencial o sensible. Enviament o traspàs segur d'informació a tercers. Congruència amb la classificació de la informació.
Riscos a mitigar	Riscos concrets: : ID5 - ID6 - ID16 - ID17 - ID18 - ID19 - ID26 - ID32 - ID33 - ID35 - ID41 - ID53 - ID69 - ID72 - ID74 Principals riscos: Robatori/fuita dades - Pèrdua d'informació - Robatori maquinari - Atac hacker
Controls ISO relacionats	10 - 11.2.7 - 12.3 - 13.1 - 18.1

Desenvolupament

El robatori o fuita d'informació és un altre dels principals riscos que pot afectar a l'Empresa X. La forma en la que es materialitzi aquest risc pot ser diversa però les conseqüències poden ser molt greus per a la imatge de l'organització i la confiança que tant els clients com els proveïdors de l'empresa dipositen en aquesta quan li cedeixen les seues dades.

Per aquest motiu, per tal d'evitar o reduir la materialització d'aquest risc, es proposa com a projecte el desenvolupament d'una Política de xifrat de dades a utilitzar per tots els empleats de l'Empresa X.

Aquesta política determinarà:

- El tipus d'informació que s'ha de xifrar de forma obligatòria.
- En quins escenaris hem de xifrar les dades: enviament per correu electrònic, còpia en suport extraïbles o dispositiu mòbil, etc.
- El procediment a emprar a l'hora de xifrar les dades.
- L'eina a utilitzar per dur a terme el xifrat: es proposa per la seua simplicitat utilitzar l'eina Gpg4win que és gratuïta i permet signar i xifrar tant correus electrònics com arxius amb clau pública.

Aquest projecte està relacionat amb el Pla de Formació, ja que part de la formació i conscienciació que s'impartirà com a sessió als treballadors

són els avantatges d'utilitzar el xifrat per a protegir la informació adientment.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, Responsable d'Infraestructures, del Director d'Infraestructures, del Responsable de Seguretat i el Comitè de Direcció.

El Responsable Tècnic junt al Responsable de Seguretat, s'encarregaran de decidir quina eina de xifrat és la més idònia per utilitzar a nivell corporatiu i de desenvolupar la política de xifrat de dades amb els corresponents procediments d'utilització del xifrat i mesures de seguretat associades amb el xifrat de dades.

El Director d'Infraestructures supervisarà el desenvolupament de la Política i presentarà el projecte davant el Comitè de Direcció.

El Comitè de Direcció donarà el vist i plau al projecte i informarà a tota l'empresa del seu suport a la implantació d'aquesta política.

Una vegada la política està consensuada i aprovada, un treballador del Departament d'Infraestructures serà l'encarregat d'instal·lar i configurar l'eina en els dispositius corporatius.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini de dos mesos.

En qualsevol cas, aquesta Política de Xifrat de dades serà tractada com una acció continua i per tant, anirà actualitzant-se i evolucionant segons les necessitats de l'Empresa X.

Quantificació econòmica

- Hores treballador (70h aprox. a 12€/h): 840€
- Hores Responsable Tècnic (100h aprox. a 20€/h): 2000€
- Hores Responsable Seguretat (100h aprox. a 30€/h): 3000€
- Hores Director d'Infraestructures (2h aprox. a 40€/h): 80€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 6100€

5.9 Millora de la Política de còpies de seguretat.

Taula Resum

Definició	**La integritat i disponibilitat de la informació que manipula**

	l'empresa és crítica i fonamental per dur a terme els processos de negoci adientment. També és gaire probable la seua pèrdua, modificació, eliminació o d'error d'accés per diversos motius.
Objectius	Millorar la política de còpies de seguretat existent per a incloure informació crítica de la que no s'està fent còpia i optimitzar el procés de còpia i recuperació d'informació en sí mateix.
Beneficis	Disponibilitat de la informació. Preservació de la integritat de la informació. Possibilitat de restauració de la informació, si escau.
Riscos a mitigar	Riscos concrets: Qualsevol risc que suposi o impliqui una pèrdua, modificació, robatori o no disponibilitat de la informació. Principals riscos: Atac hacker - No disponibilitat informació - Pèrdua d'informació - Robatori/fuita dades
Controls ISO relacionats	12.3

Desenvolupament

Aquest projecte es proposa com una millora de la política de còpies de seguretat que l'empresa ja té implantada. Encara que la funcionalitat bàsica està coberta amb la política actual, es troben mancances a nivell de seguretat que és necessari resoldre.

Amb aquest projecte s'aconseguirà una major fiabilitat quant a la disponibilitat de la informació de l'empresa i la reducció del temps de recuperació en cas de pèrdua, robatori o destrucció de dades.

La primera millora consisteix en comprar una llibreria de còpies amb la que poder fer les còpies de tots els sistemes de forma més ràpida i fàcil.

Es compraran més cintes LTO per tal de començar una rotació de cintes a l'hora de fer les còpies i allargar tant el temps de vida d'aquestes com la qualitat de les còpies.

S'actualitzaran les dades que es copien i com es copien, introduint còpies incrementals i/o diferencials, segons el tipus de dades i la seua criticitat.

S'afegiran a les còpies de seguretat els snapshots de les màquines virtuals de l'organització.

A més, cada setmana és farà una còpia de la informació i els snapshots de les màquines virtuals més crítiques per l'empresa en un grup de cintes LTO que s'enviarà fora de l'empresa.

Tota la informació inclosa en aquestes còpies es xifrarà mitjançant l'opció de xifrat AES que proporciona el programari de còpies empleat, per tal de preservar la informació i protegir-la correctament quan surti de les oficines de l'Empresa X.

Mitjançant aquest projecte s'assegura la disponibilitat de la informació i la millora en el procediment de còpies de l'empresa.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, de dos treballadors del Departament d'Infraestructures, el Responsable d'Infraestructures, del Director d'Infraestructures i el Comitè de Direcció.

El Responsable Tècnic, s'encarregarà de decidir quin tipus de llibreria i de cintes LTO comprar i instal·lar, així com de demanar pressupost a diferents proveïdors.

El Director d'Infraestructures, supervisarà els pressuposts i junt amb el Responsable Tècnic seleccionarà al proveïdor més adequat. També presentarà el projecte davant el Comitè de Direcció.

El Comitè de Direcció donarà el vist i plau al projecte i el dotarà dels recursos necessaris per a la seua implantació.

Una vegada comprat el material necessari, els dos treballadors del Departament d'Infraestructures s'encarregaran d'instal·lar i configurar la llibreria i les còpies de seguretat.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini d'un mes.

Quantificació econòmica

- Llibreria de còpies HP MSL4048: 3000€
- 50 Cintes HP LTO Ultrium: 2250€
- Hores Responsable Tècnic (24h aprox. a 20€/h): 480€
- Hores 2 treballadors instal·lació i configuració (24h aprox. a 12€/h): 576€
- Hores Director d'Infraestructures (2h aprox. a 40€/h): 80€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 6566€

5.10 Millora de l'entorn virtual corporatiu

Taula Resum

Definició	**L'entorn virtual emprat per l'Empresa X constitueix uns dels fonaments de l'organització a l'hora de desenvolupar els seus processos de negoci. Aquest entorn gestiona quasi totes les màquines crítiques de l'empresa així com les dades necessàries per dur a terme les tasques diàries. Per aquest motiu, és necessari invertir en millorar la qualitat, el rendiment i la**

	eficiència d'aquesta eina.
Objectius	Reduir el risc de no disponibilitat de la informació corporativa i al millorar el rendiment de les màquines virtuals corporatives i l'accés a les dades que gestionen.
Beneficis	Millora de la rapidesa en accés a dades. Augment de la capacitat de l'entorn virtual. Redundància en els diferents elements que composen l'entorn.
Riscos a mitigar	Riscos concrets: ID22 - ID27 - ID30 - ID45 - ID48 - ID49 - ID51 Principals riscos: No disponibilitat d'informació
Controls ISO relacionats	12.1.3 - 17.2

Desenvolupament

Per reduir el risc de no disponibilitat de la informació i al mateix temps millorar el rendiment de les màquines virtuals corporatives i l'accés a les dades que gestionen, es proposa millorar l'entorn virtual de l'Empresa X.

Aquesta millora està basada en implantar un entorn SAN, integrat per:

- Dos servidors HP Blade nous que s'integraran en un clúster d'alta disponibilitat nou que substituirà l'actual.
- Compra i configuració d'una SAN HP MSA 2040 amb tots els components necessaris per la seua instal·lació.
- 15 discos durs de 1TB. 200*15
- Migració de dades de l'entorn actual a l'entorn SAN.
- Serveis de compra, instal·lació en rack i configuració per part dels propis treballadors del Departament d'Infraestructures.

Personal necessari

Per dur a terme aquest projecte serà necessària la participació, a nivell intern, de tres treballadors del Departament d'Infraestructures, el Responsable d'Infraestructures, del Director d'Infraestructures i el Comitè de Direcció.

El Responsable Tècnic, s'encarregarà de decidir quin model de servidors i entorn SAN es més adient així com de demanar pressuposts a diferents proveïdors i de definir els procediments de migració de dades i màquines virtuals entre els dos entorns.

El Director d'Infraestructures, supervisarà els pressuposts i junt amb el Responsable Tècnic seleccionarà al proveïdor més adequat. També presentarà el projecte davant el Comitè de Direcció.

El Comitè de Direcció donarà el vist i plau al projecte i el dotarà dels recursos necessaris per a la seua implantació.

Una vegada comprat el material necessari, els tres treballadors del Departament d'Infraestructures s'encarregaran d'instal·lar i configurar els

servidors i la SAN nous, a més de fer la migració de dades i màquines virtuals entre l'entorn actual i el nou.

Planificació temporal

Aquest projecte pot implantar-se en un període de temps curt. Es considera que el projecte en la seua totalitat, pot estar implantat en un termini de tres mesos, incloent instal·lació, configuració i fase de proves.

Quantificació econòmica

- 2 servidors HP Blade: 5400€
- HP SAN MSA 2040 + components addicionals: 12000€
- Hores Responsable Tècnic (60h aprox. a 20€/h): 1200€
- Hores 3 treballadors instal·lació i configuració (100h aprox. a 12€/h): 3600€
- Hores Director d'Infraestructures (2h aprox. a 40€/h): 80€
- Hores Comitè Direcció(1h a 60€/h * 3 membres): 180€

Pressupost total: 22460€

5.11 Quick Wins

Després de valorar les 10 propostes de projectes, es consideren que els tres projectes que més beneficis poden aportar a l'hora de preservar la continuïtat de les activitats de l'empresa i reduir els principals riscos detectats en la fase d'Anàlisi de Riscos son:

- Desenvolupament del Pla de Continuïtat
- Millora de l'entorn virtual corporatiu
- Desenvolupament d'un Pla de Formació Continua en Seguretat de la Informació

Per aquest motiu a l'hora de definir la planificació temporal d'implantació dels diferents projectes proposats, aquests tindran prioritat sobre els demés.

5.12 Planificació temporal

A continuació es detalla per a cadascun dels projectes proposats quina serà la seua planificació temporal per a la seua posada en marxa en l'Empresa X.

Aquesta planificació té l'abast de dos anys per motius econòmics i de disponibilitat de personal.

Projecte	Duració	Començament	Fi
Pla de Continuïtat	6 mesos	Gener 2015	Juny 2015
Millora de l'entorn virtual	3 mesos	Març 2015	Maig 2015
Pla de Formació	12 mesos	Gener 2015	Desembre 2015
Condicionament CPD	1.5 mesos	Juliol 2015	Agost 2015
Millora de la Política de còpies de seguretat	1 mes	Octubre 2015	Octubre 2015
Línia de connexió a Internet de backup	0.5 mesos	Desembre 2015	Desembre 2015
Control d'accés digital al CPD	0.75 mesos	Gener 2016	Gener 2016
Millora de la seguretat física de l'empresa	0.75 mesos	Febrer 2016	Febrer 2016
Política de xifrat de dades	2 mesos	Març 2016	Abril 2016
Política de Classificació i Etiquetat de la Informació	4 mesos	Maig 2016	Agost 2016

6. Presentació de Resultats i entrega d'Informes

Una vegada finalitzat el desenvolupament del Pla Director de Seguretat en l'Empresa X i realitzada la implantació del SGSI derivat d'aquest, s'ha fet una avaluació de l'estat de l'Empresa X quant a seguretat de la informació.

A partir d'aquesta avaluació, es fa una presentació de resultats que es concreta en els següents documents:

- Resum executiu: Annex C d'aquest document.
- Presentació de resultats en format PowerPoint: Arxiu adjunt a aquesta memòria.
- Presentació de resultats en format video: Arxiu adjunt a aquesta memòria.

7. Conclusions

Com a conclusions finals, després de la implantació del SGSI i l'avaluació dels resultats estrets de totes les fases anteriors, es considera que mitjançant el desenvolupament i implantació d'aquest SGSI, l'Empresa X ha aconseguit millorar substancialment el seu nivell de Seguretat.

A més, mitjançant posteriors cicles de millora, manteniment i actualització, aquest SGSI pot ser proposat per a una auditoria de certificació oficial sota l'estàndard ISO/IEC 27001:2013.

Objectius aconseguits:

- Compromís de la Direcció de l'empresa en matèria de Seguretat de la Informació.
- Identificació dels actius i processos de negoci crítics de l'empresa, així com dels principals riscos que poden afectar-los.
- Valoració acurada i objectiva de l'estat de l'empresa quant a seguretat de la informació, tant en la fase prèvia al començament d'aquest projecte com en la fase final del mateix. Fent possible mesurar la millora obtinguda amb la implantació i desenvolupament del SGSI.
- Implicació de tot el personal de l'empresa en la millora del nivell de seguretat de la informació.
- Implantació de projectes orientats a protegir els actius i processos de negoci i a millorar la seua eficiència i robustesa.
- Implantació d'una cultura de seguretat en la forma de treballar de l'empresa i de gestionar els seus actius d'informació.
- Diferenciació positiva i objectiva front a altres empreses competidores del mateix sector, obtenint una millor imatge corporativa i al mateix temps afavorint la confiança dels clients.

Propostes de millores futures:

- Desenvolupament d'una Política de Dispositius mòbils.
- Definició d'una Política de Desenvolupament Segur de Programari.
- Formació específica en metodologies segures de desenvolupament de codi.
- Implantació d'una eina de Gestió Documental.
- Desenvolupament d'una Política de configuració i actualització del Firewall i Proxy.
- Desenvolupament d'un procediment d'actualitzacions en els sistemes crítics.
- Instal·lació d'extintors addicionals a les oficines de l'empresa.

8. Bibliografia

Documentació de l'assignatura Sistemes de Gestió de la Informació del Màster MISTIC. Setembre 2012.

Publicacions oficials sobre la ISO/IEC27001:2013 i ISO/IEC27002:2013

http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/

9. Annex A: Sistema de Gestió Documental

En aquest annex, s'inclouen els documents desenvolupats com a part del Sistema de Gestió Documental del SGSI de l'Empresa X.

Aquesta documentació es composa dels següents documents:

- 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

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

La Direcció de l'Empresa X ha decidit adoptar un conjunt de mesures per a protegir els actius estratègics de la companyia. Entre aquests actius es troben la informació, els documents, les plataformes i els sistemes d'informació que permeten el seu tractament, emmagatzemament, comunicació i explotació, fonamentals per al desenvolupament de les activitat de negoci i el futur de l'organització.

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és definir un marc referencial i les bases quant a Seguretat de la Informació a aplicar per l'Empresa X en la planificació i desenvolupament dels seus processos de negoci així com de les tasques i procediments inclosos dins aquests processos.

Àmbit d'aplicació

Aquesta política és d'aplicació per tot el personal de l'Empresa X així com a tot actiu d'informació que l'empresa posseeixi actualment o en el futur, de forma que la no inclusió explícita en el present document, no constitueixi argument per no protegir actius d'informació que es troben en altres formats.

Aquesta política inclou en el seu abast tota informació impresa o escrita en paper, emmagatzemada electrònicament, tramesa per correu o utilitzant mitjans electrònics, mostrada en gravacions o parlada en una conversa.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Personal de l'empresa:

  - Executa les accions correctives derivades de les auditories del SGSI
  - Sol·licita la realització d'auditories de seguretat, si escau
- Personal a càrrec de la gestió dels sistemes d'informació:
  - Realitza les auditories periòdiques o extraordinàries
  - Redacta els informes d'auditoria
  - Executa les accions correctives derivades de les auditories
- Responsable de Seguretat
  - Revisa i aprova els informes emesos com a resultat de les auditories
  - Aprova les accions correctives a executar
- Comitè de Direcció
  - Aprova l'informe de resultats de l'auditoria SGSI

Descripció

La Direcció de Empresa X reconeix el rol de la Seguretat de la Informació a l'hora d'assegurar un tractament correcte de la informació que gestiona per dur a terme les seues activitats. Els sistemes d'informació i els equips informàtics recolzen totes les funcions de l'Organització i són essencials per a poder desenvolupar els seus processos de negoci.

La pèrdua de confidencialitat, integritat o disponibilitat de la informació pot convertir-se en un perjudici per al correcte desenvolupament de les activitats de l'empresa i la seua estratègia de negoci. A més, la fuita o revelació no autoritzada d'informació pot danyar la imatge corporativa i traduir-se en una pèrdua econòmica.

Per tal de mitigar aquests riscos, la Seguretat de la Informació ha de ser una part integral de la gestió de la informació, tant si aquesta es troba en format electrònic com en format físic.

La Direcció de l'Empresa X es compromet a protegir la seguretat de la seua informació i dels sistemes que la emmagatzemen amb la intenció d'assegurar:

- la integritat de la informació, per tal que aquesta sigui acurada i actualitzada
- la disponibilitat d'aquesta per aquells que la necessiten
- la confidencialitat es preserva, per tal que la informació sigui accedida sols per aquells que tenen autorització
- l'empresa compleix tots els requeriments legals vigents

Amb la finalitat de complir aquests propòsits, l'Empresa X es compromet a implementar els controls de seguretat necessaris tal i com s'especifiquen en els estàndards ISO/IEC27001:2013 i ISO/IEC27002:2013.

La Direcció de l'Empresa X es compromet a proporcionar als seus treballadors la educació, capacitació i coneixements de seguretat necessaris per afermar l'enteniment de la importància de la seguretat de la informació i desenvolupar un tractament acurat quan estiguin treballant amb informació confidencial.

Amb el propòsit de garantir i gestionar la continuïtat del negoci de l'empresa, s'establiran les mesures i controls adients.

Aquesta política ha de ser comunicada, coneguda i respectada per tot el personal que treballi en o per l'Organització així com tercers amb qualsevol tipus d'accés a la dita informació.

Tots els empleats són responsables de reportar i enregistrar qualsevol violació de la seguretat.

S'investigarà i es sancionarà qualsevol violació a aquesta política o a qualsevol altra política o procediment del SGSI.

Control

El responsable de dur a terme el control d'aquesta política de seguretat serà el Responsable de Seguretat junt amb la Direcció de l'Empresa X.

Aquest control es farà mitjançant un seguiment periòdic i amb les revisions, millores i adaptacions que calguin.

Política d'Utilització del Correu Electrònic

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és un marc d'utilització del servei de correu electrònic proporcionat per l'Empresa X.

L'objectiu és establir unes normes, procediments i bones pràctiques respecte d'aquest servei, així com els procediments adients de gestió d'usuaris.

Àmbit d'aplicació

Aquesta política aplica a tot el personal de l'Empresa X.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Personal de l'empresa:
  - Utilització del servei seguint les normes i bones pràctiques establertes
  - Informa de la utilització incorrecta, incidències o anomalies detectades en el servei
- Personal a càrrec del servei:
  - Implantació i configuració del servei tenint en compte els requisits quant a seguretat de la informació
  - Supervisió i monitorització de l'ús adient del servei mitjançant els controls i indicadors implantats.
  - Recollir evidències quant a l'ús incorrecte del servei i informar als responsables adients
- Responsable de Seguretat
  - Revisa i aprova els informes emesos com a resultat dels seguiments i les auditories realitzades a aquest servei
  - Aprova les accions correctives a executar

Descripció

L'Empresa X gestiona tots els serveis baix el domini "empresax.es".

Cada empleat tindrà accés a un compte nominal de correu i a més formarà part de diferents llistes de distribució a nivell departamental o organitzatiu.

L'accés al compte de correu electrònic es realitzarà mitjançant el client d'escriptori de Lotus Notes o mitjançant la seua interfície web.

Els usuaris són responsables de totes les activitats realitzades amb els comptes de correu proporcionats.

Aquesta responsabilitat s'estén a tots els recursos que integren el compte i particularment a elements com la contrasenya d'accés.

Si es sospita que el compte ha esta utilitzat per una tercera persona, s'ha d'avisar immediatament al Responsable de Seguretat de la Informació de l'Organització.

Queda prohibida la suplantació d'identitat mitjançant l'enviament de missatges de correu.

Determinades pràctiques estan catalogades com abús del servei i poden causar un greu impacte en la imatge de l'empresa. Queda prohibit l'ús del compte de correu per enviar missatges com: contingut inadequat, en nom de l'empresa a través de canals no autoritzats, difusió massiva o spam, atacs de denegació de servei.

Els comptes corporatiu no poden ser emprats com a correu personal. Es permetrà un ús raonable en aquest sentit però sempre que no afecti als processos de negoci de l'Empresa X.

Control

El responsable de dur a terme el control d'aquest servei serà el Responsable de Seguretat junt amb el responsable designat al Departament d'Infraestructures.

Aquest control es farà mitjançant un seguiment periòdic i amb les revisions, millores i adaptacions del servei que calguin.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és un marc d'utilització de tots els serveis en xarxa proporcionats per l'Empresa X.

L'objectiu d'aquest document és establir unes normes, procediments i bones pràctiques respecte d'aquests serveis, així com els procediments de gestió i accés a aquests recursos.

Àmbit d'aplicació

Aquesta política aplica a tot el personal de l'Empresa X.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Personal de l'empresa:
  - Utilització dels serveis seguint les normes i bones pràctiques establertes
  - Informa de la utilització incorrecta, incidències o anomalies detectades en els serveis
- Personal a càrrec dels serveis:
  - Implantació i configuració dels serveis tenint en compte els requisits quant a seguretat de la informació
  - Supervisió i monitorització de l'ús adient d'aquests mitjançant els controls i indicadors implantats.
  - Recollir evidències quant a l'ús incorrecte dels serveis i informar als responsables adients
- Responsable de Seguretat
  - Revisa i aprova els informes emesos com a resultat dels seguiments i les auditories realitzades als serveis
  - Aprova les accions correctives a executar

Descripció

Els recursos en xarxa de l'empresa tenen com finalitat servir de suport al desenvolupament dels processos de negoci d'aquesta. No està permesa la utilització d'aquests recursos amb finalitat recreativa o personal.

Els usuaris es comprometen a respectar la configuració dels equips de treball que utilitzen, emprant únicament els programes instal·lats i demanant autorització per la instal·lació de maquinari o programari addicional així com els permisos d'accés configurats a aquests recursos. Si es necessari l'accés a altra informació o recurs per desenvolupar el seu treball, es demanarà autorització al seu responsable directe.

La transmissió d'informació per Internet no sempre es segura. Els nivells de seguretat a aplicar dependran de l'usuari i la pèrdua d'informació serà la seua responsabilitat.

Tots els equips contenen informació confidencial i estan connectats a sistemes interns en xarxa, per tant, hauran d'estar configurats amb un sistema de control d'accés amb contrasenya aprovat pel Responsable de Seguretat de la Informació.

A més, tots els equips hauran d'estar configurats perquè es bloquegin després d'un temps d'inactivitat.

Les connexions a l'ERP intern que estiguin inactives durant un temps determinat es tallaran sent necessari tornar a connectar-se mitjançant usuari i contrasenya.

El programari instal·lat als equips ha de ser registrat prèviament per a l'ús de l'empresa. Queda prohibit utilitzar còpies de programari o documentació il·legal o il·legítima.

La utilització incorrecta dels recursos en xarxa pot entorpir el treball d'altres persones o ocasionar despeses innecessàries. Per tant, s'ha d'evitar la utilització indiscriminada de vídeos, música o imatges, ja que poden saturar la connexió d'Internet.

Els usuaris són responsables de totes les activitats realitzades amb els comptes d'usuari assignats.

Aquesta responsabilitat s'estén a tots els recursos que integren els sistemes d'informació de l'empresa i particularment a elements com la contrasenya d'accés.

Si es sospita que s'està fent un ús inadequat de qualsevol recurs corporatiu en xarxa, s'ha d'avisar immediatament al Responsable de Seguretat de la Informació de l'Organització.

Queda prohibida la suplantació d'identitat mitjançant l'inici de sessió amb credencials alienes.

Control

El responsable de dur a terme el control d'aquests serveis serà el Responsable de Seguretat junt amb els responsables designats al Departament d'Infraestructures.

Aquest control es farà mitjançant un seguiment periòdic i amb les revisions, millores i adaptacions dels serveis que calguin.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és descriure els processos a aplicar per l'Empresa X en la planificació, elaboració i execució d'auditories internes dins de l'empresa, tant del SGSI implantat com auditories tècniques que garanteixin periòdicament la integritat, disponibilitat i confidencialitat dels recursos corporatius i la millora continua del SGSI.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Personal de l'empresa:
  - Executa les accions correctives derivades de les auditories del SGSI
  - Sol·licita la realització d'auditories de seguretat, si escau
- Personal a càrrec de la gestió dels sistemes d'informació:
  - Realitza les auditories periòdiques o extraordinàries
  - Redacta els informes d'auditoria
  - Executa les accions correctives derivades de les auditories
- Responsable de Seguretat
  - Revisa i aprova els informes emesos com a resultat de les auditories
  - Aprova les accions correctives a executar
- Comitè de Direcció
  - Aprova l'informe de resultats de l'auditoria SGSI

Descripció

Tots els membres de l'equip d'Auditories Internes han de ser designats pel Responsable de Seguretat.

A l'hora de designar l'equip d'Auditories internes, únicament el personal intern competent i independent que no estigui directament relacionat amb l'àrea objecte de l'auditoria, podrà realitzar-les.

Pot donar-se el cas que el Responsable de Seguretat actuï com a Auditor Cap, donat la grandària de l'empresa i depenent de la disponibilitat i aptitud dels recursos disponibles.

L'Auditor Cap designat supervisarà l'activitat de l'equip auditor.

L'Auditor Cap haurà de preparar una auditoria interna anual del SGSI. Aquesta haurà de ser aprovada prèviament per la Direcció de l'Organització. El seu objectiu o propòsit serà revisar l'estat del SGSI per tal de reflectir qualsevol canvi en les prioritats o planificació durant l'any.

Si es considera necessari es podran dur a terme auditories no programades.

A partir del programa d'auditoria, l'Auditor Cap haurà de preparar els respectius plans o notificacions d'auditoria.

Aquests plans o notificacions hauran de ser revisats i aprovats pel Responsable de Seguretat. Hauran de ser comunicats als auditors i als auditats. Seran dissenyats per a ser flexibles i permetre canvis basats en la informació recollida durant l'auditoria. Els plans hauran d'incloure:

- L'abast i objectiu de l'auditoria
- Departament i responsable a càrrec
- Membres de l'equip auditor
- Data, lloc i hora de l'auditoria
- Data d'entrega de l'informe d'auditoria

Es realitzarà una reunió abans de l'auditoria entre el Responsable de Seguretat, l'Auditor Cap i l'equip auditor per confirmar la disponibilitat dels recursos necessaris per dur a terme l'auditoria i al mateix temps per verificar l'abast de l'auditoria.

El dia de l'auditoria, abans de començar aquesta, es realitzarà una reunió d'apertura on es tractaran temes com el propòsit i abast de l'auditoria, es confirmarà el pla d'auditoria i s'esclariran els dubtes necessaris.

Quan comenci l'auditoria, l'equip auditor utilitzarà diferents llistes de comprovació per dur a terme les comprovacions corresponents: particulars al departament o procés auditat, relatius a requeriments específics de la norma ISO/IEC27001 i a controls inclosos en la norma ISOC/IEC27002.

Durant l'auditoria es realitzaran entrevistes, s'examinaran documents i diverses activitats i condicions seran observades per tal de recollir les evidències necessàries en les que basar l'informe final d'auditoria.

L'***Informe d'Auditoria*** serà preparat per l'Auditor Cap i ha d'incloure la següent informació:

- Nombre de referència de l'auditoria
- Data en la que s'ha realitzat aquesta
- Departament o procés auditat
- Nom del responsable auditat i dels auditors
- Llistat de les evidències i no conformitats trobades
- Accions correctores i preventives associades

Aquest informe serà entregat al Responsable de Seguretat en cas de que aquest no sigui també l'Auditor Cap i aquest serà l'encarregat de mantenir i guardar aquest informe.

Control

El responsable de dur a terme el control de les auditories internes serà el Responsable de Seguretat.

Aquest control es farà en dos nivells diferents, mitjançant un seguiment periòdic i amb les auditories periòdiques necessàries.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és seleccionar i establir els indicadors necessaris per a controlar el funcionament de les mesures de seguretat de la informació implantades o a implantar a l'Empresa X, d'avaluar l'eficiència i eficàcia de les mateixes i de supervisar l'evolució de l'estat de la Seguretat de la Informació.

Aquests d'indicadors també poden ajudar a mesurar la rendibilitat de les inversions realitzades en matèria de Seguretat en l'Empresa X.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

NIST 800-30. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.

Responsabilitats

- Personal a càrrec de la gestió dels sistemes d'informació:
  - Implantació i manteniment dels indicadors
  - Mesurament i avaluació dels resultats
- Responsable de Seguretat
  - Revisa i aprova els informes emesos com a resultat de les avaluacions i mesuraments dels indicadors
  - Proposa i aprova els indicadors a implantar
- Comitè de Direcció
  - Aprova l'informe de resultats de l'avaluació d'indicadors

Descripció

S'han de definir els mecanismes i la periodicitat de mesura dels indicadors establerts.

Tots els indicadors tindran definits aquests components bàsics:

- Nom: Significatiu.
- Descripció: Objectiu de mesura.
- Control a que dona suport.
- Freqüència de mesura.
- Valor llindar.

El mesurament dels indicadors establerts haurà de ser fiable i repetible i estarà basat en evidències objectives.

A continuació, es mostra un llistat dels indicadors seleccionats i la forma en la que es mesura cadascun.

ID	*Indicador*	*Mesura*
1	Revisions de la Direcció	Registres i actes de reunió signades pel Comitè de Direcció quant a revisions del SGSI.
2	Treballadors que han signat el contracte de confidencialitat	Nº total de treballadors que han signat/ Nº total de treballadors
3	Dispositius mòbils amb antivirus instal·lat	Nº total de mòbils corporatius amb antivirus/ Nº total de mòbils corporatius
4	Verificació de credencials	Comprovació del CV dels nous treballadors/Nº contractes anuals
5	Sessions formació impartides	Registre de comprovació de les sessions de conscienciació sobre seguretat de la informació impartides en l'empresa així com dels empleats assistents
6	Usuaris no deshabilitats en el domini	Nº usuaris no deshabilitats/Nº de baixes de treballadors
7	Actius no etiquetats	Registres i informes d'auditories que reflecteixen no conformitats quant a la classificació i etiquetat d'informació
8	Incidències amb suports extraïbles	Registres d'incidències relacionades amb suports extraïbles: gestió, eliminació o utilització
9	Incidències de control d'accés en els servei en xarxa	Registres d'incidències relacionades amb el control d'accés en els serveis en xarxa corporatius
10	Revisions permisos d'accés d'usuaris	Registres i informes de les revisions realitzades pel Dep. d'Infraestructures dels permisos d'accés dels usuaris del domini
11	Autogestió de contrasenyes	Nº d'incidències ateses sobre gestió de contrasenyes

ID	*Indicador*	*Mesura*
12	Equips sense control d'accés	Nº equips de treball/portàtils/mòbils sense control d'accés amb contrasenya
13	Revocació de claus	Nº de claus revocades/Nº baixes d'usuari amb clau assignada
14	Robatori d'actius	Nº de robatoris d'actius, tant els efectius com els intents
15	Entrada en funcionament del SAI	Nº d'entrades en funcionament SAI.
16	Procediments d'operació no documentats	Nº de procediments d'operació establerts sense documentació associada
17	Equips desactualitzats o sense antivirus	Nº d'equips de treball/portàtils/mòbils sense antivirus o amb ell però no actualitzat
18	Percentatge còpies fallides	(Nº còpies fallides/Nº còpies totals)*100
19	Modificació o eliminació d'esdeveniments	Registres de les auditories automatitzades en el sistema
20	Rollbacks realitzats en servidors corporatius	Nº de procediments de marxa enrere duts a terme en els servidors corporatius
21	Vulnerabilitats de criticitat alta	Nº de vulnerabilitats amb criticitat alta detectades amb escanejos d'eines com Nessus, Nikto o similar
22	Autoritzacions auditories	Nº de registres d'autorització d'auditories signades per Direcció/Nº total auditories
23	Autenticacions fallides al iniciar sessió en el correu web	Nº de bloquejos d'un usuari al intentar iniciar sessió en la interfície web de Notes
24	Incompliments política d'intercanvi d'informació	Nº de registres d'incompliments o no conformitats de la política d'intercanvi d'informació
25	No conformitats en requisits de seguretat de la informació	Registres de no conformitats emesos en les auditories realitzades
26	Accessos no autoritzats al mòdul de Nòmines de l'ERP	Registres i no conformitats emeses en auditories sobre accessos no autoritzats al mòdul de Nòmines de l'ERP corporatiu
27	Incompliments de contracte per part de tercers	Registres d'incidències o incompliments de contracte en la prestació de servei o gestió d'informació d'un tercer
28	Revisions de condicions de contracte amb tercers	Registres de les revisions de contracte signades pel Dep. d'Administració, per actualitzar-los o adaptar-los a nivell regulatori o de condicions de servei
29	Percentatge de resolució d'incidències	(Nº d'incidències solucionades/Nº d'incidències obertes)*100
30	Activació de plans de contingència	Nº d'activació de plans de contingència
31	Caigudes de sistemes	Nº de caigudes dels sistemes d'informació per falta d'elements redundants (per sistema)
32	No conformitats detectades en auditories LOPD	Nº de no conformitats detectades en la última auditoria respecte la LOPD i RDLOPD
33	No conformitats detectades en les polítiques i estàndards de seguretat	Nº de no conformitats detectades en la última auditoria del SGSI

El detall sobre els indicadors implantats o a implantar i la seua relació amb els controls de la ISO/IEC 27002:2013, es troba a l'arxiu adjunt "BorregoRodriguezPatricia_Gestió Indicadors_27002_2013.xlsx".

S'ha de tenir en compte que aquesta és una primera aproximació en la implantació del SGSI. Els indicadors hauran de revisar-se i actualitzar-se com a part del cicle de millora del SGSI així com afegir o modificar indicadors segons sigui necessari.

Control

El responsable de dur a terme el control de l'aplicació dels indicadors seleccionats, el seu funcionament i el correcte mesurament de cadascun d'aquests, serà el Responsable de Seguretat.

Aquest control es farà en dos nivells diferents, mitjançant un seguiment periòdic i amb les auditories periòdiques necessàries.

Procediment de Revisió per Direcció

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és definir el procediment a dur a terme per part de la Direcció de l'Empresa X en les tasques de revisió i supervisió del correcte funcionament del SGSI implantat.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Responsable de Seguretat
  - Presentar a la Direcció els informes emesos com a resultat de les diferents avaluacions, revisions i auditores realitzades
  - Justificar i explicar els detalls dels informes
- Comitè de Direcció
  - Revisió periòdica de l'estat del SGSI

Descripció

La Direcció General de l'Empresa X ha de revisar el Sistema de Gestió de la Seguretat de la Informació de l'Organització, com a mínim de manera anual, per tal d'assegurar la seua idoneïtat, adequació i efectivitat.

Si es considera necessari es podran convocar revisions no planificades.

La informació que es tractarà en aquesta revisió permetrà que la Direcció tingui una visió general de:

- L'estat de les accions establertes en revisions prèvies realitzades per la Direcció
- Els canvis, tant externs com interns, que afecten i són d'importància per al SGSI
- El rendiment del SGSI mitjançant dades sobre les no conformitats i les accions correctives implantades, els resultats dels processos de monitorització i mesurament així com els resultats de les auditories realitzades i del compliment dels objectius del SGSI
- Informació important de terceres parts com clients o proveïdors
- Els resultats de l'anàlisi de riscos
- Les possibles oportunitats de millora continua

La Direcció de l'Empresa X, després d'avaluar i revisar la informació proporcionada, prendrà les decisions adients quant a les oportunitats de millora continua i qualsevol altra necessitat de canvis en el SGSI.

Es redactarà i guardarà un acta de reunió com a evidència dels resultats definits i obtinguts d'aquestes revisions.

Control

El responsable de controlar una correcta revisió del SGSI per part de la Direcció de l'organització, serà el Responsable de Seguretat.

Aquest control es farà en dos nivells diferents, mitjançant un seguiment periòdic i revisió de les actes i informes de reunió realitzades, a més de les auditories periòdiques.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és definir el procediment a dur a terme per part de la Direcció de l'Empresa X en les tasques de revisió i supervisió del correcte funcionament del SGSI implantat.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Responsable de Seguretat
  - Definició i assignació de Rols i Responsabilitats quant a matèria de Seguretat de la Informació
  - Justificar i explicar els detalls dels assignacions
- Comitè de Direcció
  - Aprovar la definició i assignació de Rols i Responsabilitats

Descripció

El Comitè de Direcció de l'Organització és l'encarregat d'avaluar i aprovar les decisions estratègiques quant a la Seguretat de la Informació. Format pels tres membres de la Direcció General de l'empresa, tindrà entre les seues funcions:

- Engegar els mecanismes requerits perquè la Seguretat de la Informació s'integri dins els processos de negoci de la companyia
- Haurà de dotar a l'empresa del suport i recursos necessaris per poder abordar la implantació d'un SGSI

- Donar el seu vist i plau a polítiques en matèria de seguretat de la informació així com al pla de seguretat
- Determinar el llindar de risc acceptable en seguretat

Totes les decisions d'aquest comitè hauran de ser recollides en acta.

El Comitè de Seguretat de la Informació és l'encarregat de prendre les decisions en matèria de Seguretat de la Informació de manera consensuada. Per aquest motiu, aquest Comitè haurà d'estar format per un grup de responsables representats de cadascuna de les àrees de l'Empresa X. L'objectiu d'aquest Comitè és crear, mantenir, supervisar i millorar el SGSI de l'Empresa X.

El Comitè de Seguretat de la Informació de l'Empresa X estarà format per:

- Un membre representant de la Direcció General
- El Director del Departament d'Administració
- El Director del Departament Comercial
- El Director del Departament d'Infraestructures
- El Responsable de Seguretat de la Informació

A banda d'aquests membres permanents, podran intervenir els convidats que siguin necessaris segons els temes a abordar.

Les funcions d'aquest Comitè són, entre d'altres:

- Implantar les directrius del Comitè de Direcció.
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al Comitè de Direcció de polítiques de seguretat de la informació.
- Validar el pla de seguretat de la informació
- Promoure la conscienciació i formació dels treballadors
- Revisar les incidències més crítiques
- Supervisar que es compleixi amb la legislació vigent

El Responsable de Seguretat de la Informació és un càrrec assumit per personal intern de l'Empresa X. Dins les seues funcions estan:

- La coordinació de totes les accions relacionades amb la Seguretat de la Informació en qualsevol de les seues formes i en totes les etapes de la vida d'aquesta, amb l'objectiu de protegir la seua confidencialitat, integritat i disponibilitat.

- Es responsabilitzarà tant de la seguretat a nivell lògic com a nivell físic dins de l'Empresa X.
- També serà l'encarregat de dialogar i comunicar-se amb els diferents grups de treball o equips que conformen les distintes àrees de l'Organització.

Els Directors de Departament, dins les seues respectives àrees, seran els encarregats de:

- Classificar la informació de la qual són responsables
- Conèixer la normativa aplicable a la informació de la que són responsables
- Definir els requisits de seguretat per al tractament de la informació
- Col·laborar en les revisions i auditories de seguretat de la informació.

La resta de Personal tindrà com a funcions, entre d'altres:

- Conèixer i complir les polítiques de Seguretat de la Informació
- Fer un bon ús dels sistemes i de la informació a la que tenen accés, protegint ambdós.
- Respectar les normes i procediments vigents en matèria de seguretat de la informació.
- Notificar les anomalies o incidències de seguretat per la via establerta.

Control

El responsable de controlar la gestió de rols i responsabilitats en matèria de Seguretat de la Informació i del SGSI, serà el Responsable de Seguretat.

Aquest control es farà en dos nivells diferents, mitjançant un seguiment periòdic i amb les auditories periòdiques necessàries.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és definir el procediment o metodologia a utilitzar en la realització de l'anàlisi de riscos que poden afectar als actius de l'Empresa X.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

NIST 800-30. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.

Responsabilitats

- Responsable de Seguretat
    - Definició de la metodologia d'Anàlisi de Riscos

Descripció

La metodologia escollida per dur a terme l'anàlisi de riscos en l'Empresa X es fonamenta en els següents procediments:

Identificació d'Actius: Elements a protegir propis de l'Organització i que aquesta requereix per a desenvolupar i realitzar els seus processos de negoci. Existeixen diferents tipus d'actius a tenir en compte, com:

- Actius físics: Actius de maquinari o hardware que utilitza l'empresa.

- Actius lògics: Actius de programari o software que utilitza i genera l'empresa.
- Actius de personal: Les persones des del punt de vista de rol o perfil que intervé en el desenvolupament de les tasques de l'organització.
- Actius d'infraestructura: Actius necessaris perquè la resta de l'empresa pugui funcionar correctament com l'aire condicionat o la llum elèctrica, mobiliari d'oficina, etc.
- Actius intangibles: Elements com la imatge corporativa, credibilitat, know how, etc.

Una valoració correcta dels actius tindrà en compte aspectes com el valor de reposició, de configuració, d'utilització o de pèrdua d'oportunitat així com de la informació que contenen, si escau.

Identificació d'Amenaces: Totes les situacions que poden danyar els actius i de les què s'han de protegir. L'Empresa X està exposada a una sèrie d'amenaces que són les causants dels riscos i per tant dels danys possibles.

Identificació de Vulnerabilitats: Són les diferents debilitats que presenten els actius de l'empresa. Les amenaces aprofiten les vulnerabilitats de l'Organització per a danyar els actius d'aquesta.

La sistemàtica per a calcular el risc, es basa en la relació entre actius, amenaces i vulnerabilitats.

A l'hora de calcular els riscos que poden afectar a l'Empresa X, s'utilitzarà una metodologia basada en la metodologia NIST per a dur a terme aquest càlcul.

Es determinen tres nivells diferents quant a la freqüència d'ocurrència i la criticitat de l'impacte: baix, mitjà i alt. A partir d'aquests nivells es defineix un quadre d'encreuaments que té com a resultat els diferents riscos que es poden donar en l'Organització.

Probabilitat d'amenaça	***Impacte***		
	Baix	**Mitjà**	**Alt**
Baix	Baix	Baix	Baix
Mitjà	Baix	Mitjà	Mitjà
Alt	Baix	Mitjà	Alt

Per últim, s'estableix el valor llindar dels riscos, que també es classifica en tres nivells:

- Risc Baix: S'ha d'avaluar si s'accepta el risc o si cal implantar alguna mesura de control.
- Risc Mitjà: S'han d'implantar les mesures adients per controlar aquest risc, sempre que no existeixen riscos amb nivell alt sense tractar.
- Risc Alt: S'han d'implantar les mesures de seguretat necessàries per reduir aquest risc.

Amb aquesta metodologia després d'identificar els actius i analitzar-los, s'identifiquen les vulnerabilitats que presenten cadascun d'ells i es determinen quines amenaces poden fer ús de les vulnerabilitats identificades.

A continuació, s'identifica quina característica de la seguretat de la informació quedaria afectada per cadascuna de les possibles situacions: confidencialitat, integritat i/o disponibilitat.

Per últim i sospesant tota la informació anterior s'estima la probabilitat de que aquesta situació arribi a donar-se i l'impacte que provocaria sobre l'organització, obtenint així el risc al que està exposada l'empresa.

Control

El responsable de controlar la correcta aplicació i utilització de la metodologia d'anàlisi de riscos escollida, serà el Responsable de Seguretat.

Aquest control es farà mitjançant la revisió de les anàlisi realitzades i dels seus resultats així com dels controls i projectes derivats d'aquesta anàlisi i la seua adequació a la situació tant del SGSI com de l'Empresa X.

Versió	Data	Autor	Revisat	Descripció
1.0	17/10/2014	Patricia Borrego	Responsable de Seguretat	Versió Inicial

Objectiu i Motivació

La finalitat amb la que s'emet aquest document és establir el procediment de realització de la declaració d'aplicabilitat del SGSI quant al compliment dels estàndards ISO/IEC27001:2013 i ISO/IEC27002:2013 en l'Empresa X.

Aquest document descriu els controls de la ISO/IEC27002:2013 que són objectius, rellevants i aplicables al SGSI de l'organització, basat en els resultats i conclusions de la valoració i el tractament del risc.

Àmbit d'aplicació

Aquest procediment és d'aplicació per als actius implicats en la seguretat de la informació de l'empresa, definit en l'anàlisi de riscos, els sistemes de gestió corporatius i el SGSI.

Compliment legal i d'estàndards de seguretat

ISO/IEC 27001:2013. Tecnologia de la informació. Tècniques de Seguretat. Sistemes de Gestió de la Seguretat de la Informació (SGSI). Requisits.

ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.

Responsabilitats

- Responsable de Seguretat
  - Establiment del procediment de la declaració d'aplicabilitat
- Comitè de Direcció
  - Avaluació dels resultat extrets d'aquesta declaració

Descripció

A l'arxiu adjunt amb nom "BorregoRodriguezPatricia_SOA 27002_2013_TFM_Fase2.xlsx", es detallen els controls de seguretat de la norma ISO/IEC27002:2013 que s'apliquen o es van a aplicar en l'Organització com a part del desenvolupament i implantació del Sistema de Gestió de Seguretat de la Informació en l'Empresa X.

Control

El responsable de controlar la correcta realització i supervisió de la declaració d'aplicabilitat, serà el Responsable de Seguretat.

Aquest control es farà mitjançant la revisió dels seus resultats i la seua adequació a la situació tant del SGSI com de l'Empresa X.

10. Annex B: Auditoria de Compliment

En aquest annex, s'inclou l'informe en el que es detalla tota la informació rellevant sobre l'Auditoria de Compliment del SGSI de l'Empresa X basada en l'estàndard ISO/IEC 27002:2013.

Informe d'Auditoria de Compliment del SGSI basat en l'estàndard ISO/IEC27002:2013

Desembre 2016

Versió	Data	Auditor	Descripció
1.0	05/12/2016	Patricia Borrego	Versió Inicial

Data de l'auditoria

Dilluns, 05 de Desembre de 2016, València.

Equip Auditor

La persona encarregada de dur a terme aquesta auditoria és l'auditora informàtica Patricia Borrego.

Identificació de la companyia

Aquesta auditoria es realitza en les instal·lacions de l'Empresa X, amb seu en València capital.

Objectiu

Aquest informe es realitza per encàrrec del Comitè de Direcció de l'Empresa X. Forma part de la implantació del SGSI corporatiu que es va a començar a desenvolupar en Setembre de 2014.

Dos anys després, quan teòricament s'han implantat tots els projectes de millora proposats, és necessari avaluar el grau de maduresa en seguretat que ha aconseguit l'organització i el nivell de compliment amb l'estàndard de referència.

Abast i Norma de referència

L'Abast d'aquesta auditoria de compliment inclou la totalitat del SGSI implantat en l'Empresa X, i per tant, afecta a la gestió de la seguretat de tota la informació i els sistemes que la processen i suporten per al desenvolupament dels processos de negoci de l'Empresa X.

La norma de referència que s'utilitza per dur a terme aquesta auditoria de compliment és la ISO/IEC27002:2013.

Avaluació de la maduresa

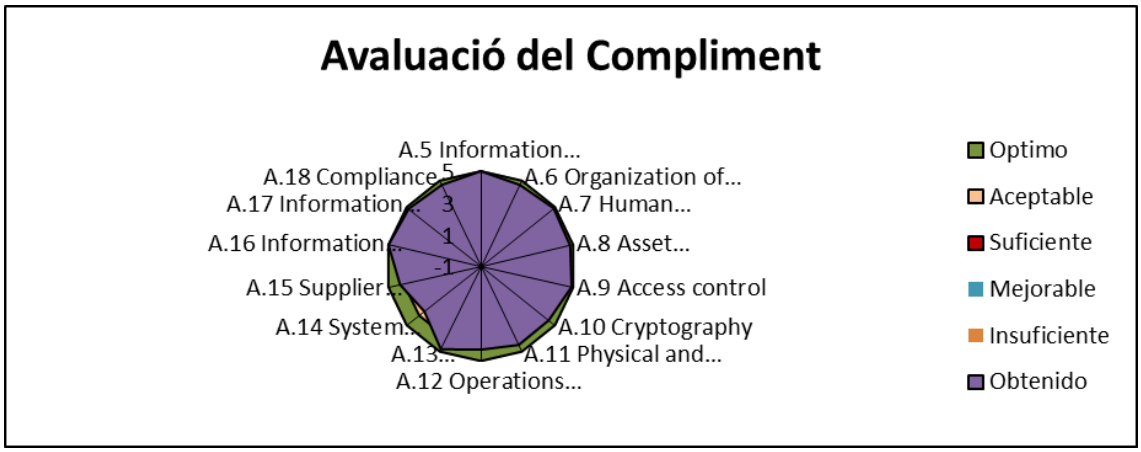
L'objectiu de realitzar aquesta auditoria de compliment és el d'avaluar el nivell d'acompliment aconseguit en matèria de Seguretat de la Informació en l'Empresa X. Després d'implantar tots els projectes proposats en el procés d'implantació del SGSI de l'organització, és necessari estimar l'estat en el que es troba l'empresa i poder fer una comparació d'aquest amb respecte l'estat inicial en el que es trobava abans de començar amb el desenvolupament del Pla Director de Seguretat.

La metodologia que s'emprarà està basada en el model SSE-CMM que defineix 6 nivells diferents, de 0 a 5, per a mesurar el grau d'implantació dels controls de seguretat.

ID	NIVELL	PRÀCTIQUES DE GESTIÓ IT
0	**NO EXISTENT**	No hi ha una definició de responsabilitats en matèria de seguretat de la informació
1	**INICIAL** (hi ha una aproximació)	Les responsabilitats principals s'assignen o assumeixen informalment. Cada persona sap la seva responsabilitat, però no la dels altres.
2	**REPETIBLE** (existeix, amb moltes deficiències)	Se sap qui assumeix les funcions principals en matèria de seguretat de les TIC i de la resta del negoci, però les funcions de seguretat no estan definides ni documentades específicament, sinó que s'assumeixen individualment com a part d'altres funcions (per exemple, la direcció d'un projecte)
3	**DEFINIT** (existeix, amb algunes deficiències)	Les responsabilitats en seguretat de la informació s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, s'han donat a conèixer i s'ha fet o planificat la capacitació de totes les persones que ho requereixin
4	**GESTIONAT** (existeix i és correcte)	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, però no es fa una revisió anual per a verificar que totes les funcions s'han assignat bé i que els responsables desenvolupen la seva funció.
5	**OPTIMITZAT** (existeix i està integrada en un cicle de millora continua)	Les responsabilitats s'han definit i documentat en tots els nivells de negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, es revisa periòdicament el desenvolupament d'aquestes funcions i hi ha un procés per a detectar deficiències en l'assignació i coordinació de funcions i per a aplicar-hi correccions

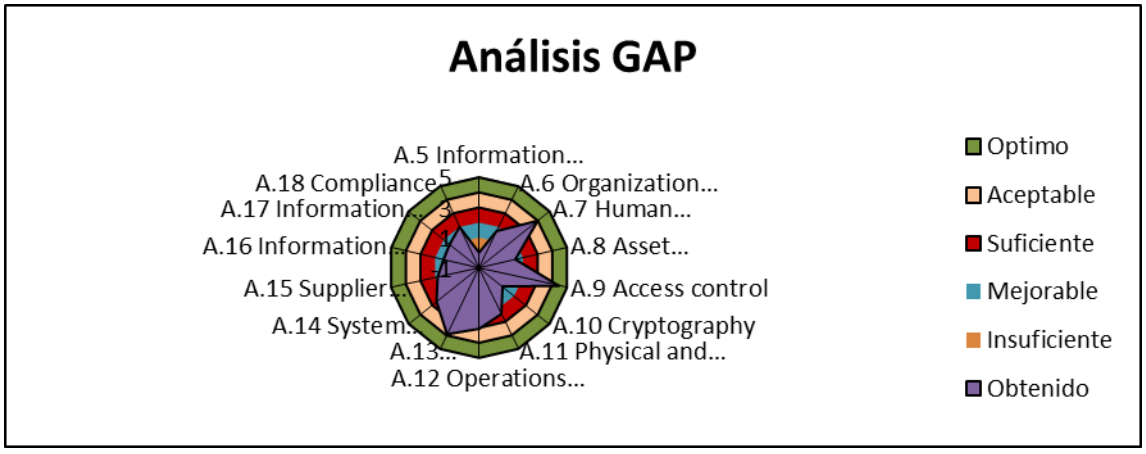
A continuació, podem veure un quadre resum de la maduresa dels controls implantats a l'Empresa X junt amb la seua gràfica associada.

	Valor
A.5 Information security policies	5
A.6 Organization of information security	4,7
A.7 Human resource security	4,89
A.8 Asset management	4,81
A.9 Access control	4,9
A.10 Cryptography	4,5
A.11 Physical and environmental security	4,53
A.12 Operations security	4,29
A.13 Communications security	4,83
A.14 System acquisition, development and maintenance	3,58
A.15 Supplier relationships	4,25
A.16 Information security incident management	5
A.17 Information security aspects of business continuity management	4,83
A.18 Compliance	4,7



En l'arxiu Excel "AudCompliment_TFM_Fase5.xls" es pot veure el desglossament de tots els controls avaluats en aquesta anàlisi diferencial.

Si fem una comparació amb l'anàlisi GAP fet abans del desenvolupament i la implantació del Pla Director de Seguretat podem comprovar com la millora en el compliment en matèria de seguretat de tots els dominis analitzats de l'estàndard ISO:IEC27002:2013 en l'organització ha sigut substancial i molt satisfactòria des d'un punt de vista global.



Desenvolupament de l'auditoria

L'equip auditor a l'hora de recaptar informació per poder avaluar la maduresa del SGSI implantat en l'Empresa X ha dut a terme les següents tasques:

- Reunió amb el Responsable de Seguretat
- Reunió amb el Responsable Tècnic
- Reunió amb el Responsable de Programari
- Reunió amb el Director del Departament d'Administració
- Reunió amb el Director del Departament de Comercial
- Entrevista amb un programador

- Entrevista amb un tècnic
- Entrevista amb un administratiu
- Entrevista amb un comercial
- Avaluació de les polítiques i procediments desenvolupats
- Avaluació dels registres d'evidències presentats per l'Empresa com a prova del compliment de les polítiques desenvolupades

Relació de No Conformitats Majors i Menors

Després d'avaluar la maduresa del SGSI implantat en l'Empresa X s'han trobat 6 no conformitats menors, 1 no conformitat major i 9 observacions.

Taula Resum de No Conformitats i Observacions per Domini ISO 27002

Domini ISO	NC Menors	NC Majors	Observacions
A.5 Information security policies	0	0	0
A.6 Organization of information security	**1**	0	0
A.7 Human resource security	0	0	**1**
A.8 Asset management	0	0	**2**
A.9 Access control	**1**	0	0
A.10 Cryptography	0	0	**1**
A.11 Physical and environmental security	0	0	**3**
A.12 Operations security	**2**	0	0
A.13 Communications security	0	0	**1**
A.14 System acquisition, development and maintenance	0	**1**	0
A.15 Supplier relationships	**1**	0	0
A.16 Information security incident management	0	0	0
A.17 Information security aspects of business continuity management	0	0	**1**
A.18 Compliance	**1**	0	0

Observant tant els resultats obtinguts en el diagrama de radar com en la taula anterior trobem que el domini "A.14 Adquisició, desenvolupament i manteniment de sistemes" és el que obté un grau menor d'acompliment o maduresa dels controls. Això també queda reflectit en la No Conformitat Major que se li ha atorgat ja que encara que a nivell procedimental ha començat a desenvolupar-se una Política de programari segur, no es troben evidències suficients com per a constatar que aquests procediments estan sent implementats i aplicats adientment.

A continuació, es descriu cadascuna de les No Conformitats Menors, Majors i Observacions:

No Conformitats Menors

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_01_051216	**TIPUS NC**	Menor	**DATA NC**	30/11/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.6.1.2	**ÀMBIT**	Organització de la informació de seguretat
ENTREVISTAT			Responsable de Seguretat		
ÀREA			Seguretat		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix un document que reculli de manera formal la segregació de deures en l'empresa.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Sistema de Gestió Documental SGSI					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
Redactar aquest document i incloure-ho com a part del SGSI després de la seua aprovació			Responsable de Seguretat		
OBSERVACIONS					
Existeix una segregació de tasques en l'empresa tant a nivell de departaments com dins de cadascun d'aquests encara que no existeix un document que reculli aquesta segregació.					

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_02_051216	**TIPUS NC**	Menor	**DATA NC**	30/11/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.9.4.4	**ÀMBIT**	Control d'accés
ENTREVISTAT			Responsable Tècnic		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix una política d'utilització de programari privilegiat que estigui aprovada per la Direcció.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de Control d'Accés del SGSI					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
Redactar aquesta política i els procediments adients derivats d'aquesta.			Responsable Tècnic		
OBSERVACIONS					
La utilització d'aquest tipus d'aplicacions és esporàdica i molt restringida. L'accés a aquest tipus d'eines està restringit al departament d'Infraestructures i és el Responsable tècnic qui ha de donar accés a aquestes eines.					

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_03_051216	**TIPUS NC**	Menor	**DATA NC**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.12.1	**ÀMBIT**	Procediments i responsabilitats operacionals
ENTREVISTAT			Tècnic i Programador		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix una política o procediment estandarditzat a l'hora de documentar els procediments operatius del departament d'Infraestructures. Encara que la gestió de canvis i de capacitats sí es realitza no sempre es documenta. No existeix un procediment formalitzat documentat per realitzar traspassos de programari o codi entre entorns de producció i proves.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política d'operacions del Departament d'Infraestructures					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
Redactar la política i els procediments necessaris quant a procediments operatius de les instal·lacions de processament d'informació, de gestió de canvis i capacitat i de traspàs d'informació entre entorns per tal de formalitzar i estandarditzar com dur a terme aquestes tasques correctament.			Responsable Tècnic i Responsable de Programari		
OBSERVACIONS					

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_04_051216	**TIPUS NC**	Menor	**DATA NC**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.12.4	**ÀMBIT**	Logging i Monitorització
ENTREVISTAT			Tècnic		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix un procediment estandarditzat sobre la gestió d'esdeveniments, l'accés i protecció dels logs o la sincronització de rellotges dels sistemes, que pot afectar a la integritat i fiabilitat dels esdeveniments que es generen. El seu tractament tampoc està optimitzat ja que els administrador tenen capacitat de modificar-los.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política d'operacions del Departament d'Infraestructures					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
Redactar els procediments de gestió d'esdeveniments i de sincronització de rellotges en els sistemes corporatius, a més d'aplicar les mesures adients per evitar la modificació dels logs.			Responsable Tècnic		
OBSERVACIONS					

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_05_051216	**TIPUS NC**	Menor	**DATA NC**	02/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.15.2.1	**ÀMBIT**	Monitorització i revisió de serveis de proveïdors
ENTREVISTAT			Director Administració		
ÀREA			Departament d'Administració		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix cap evidència de que el procediment de revisió i monitorització dels serveis proporcionats pels proveïdors s'estigui aplicant.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de proveïdors					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
És necessari implantar controls per a obtenir evidències acurades i verificables de si s'aplica o no aquest procediment			Director Administració		
OBSERVACIONS					

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_06_051216	**TIPUS NC**	Menor	**DATA NC**	02/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.18.1.2	**ÀMBIT**	Propietat de drets intel·lectuals
ENTREVISTAT					
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - NO CONFORMITAT					
Es troben eines instal·lades en els equips de treball que són il·legítimes (piratejades) o no tenen llicència.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Registre d'evidències i Política de Seguretat (compliment legal - LOPD)					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
És necessari implantar controls i procediments efectius per a evitar la utilització de programari que no sigui legal.			Responsable de Seguretat		
OBSERVACIONS					

No Conformitats Majors

NO CONFORMITATS (NC) D'AUDITORIA					
CODI NC	NC_07_051216	**TIPUS NC**	Major	**DATA NC**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.14	**ÀMBIT**	Adquisició, desenvolupament i manteniment de sistemes
ENTREVISTAT			Programador i Responsable de Programari		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - NO CONFORMITAT					
No existeix una política de desenvolupament segur de programari. No s'han desenvolupat els procediments necessaris per assegurar correctament la informació inclosa a l'ERP o el seu tractament. No es troben els documents que s'haurien d'haver generat com a resultat de dur a terme tasques concretes com modificacions o revisions.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de Seguretat SGSI					
ACCIONS CORRECTIVES			**RESPONSABLE DE RESOLUCIÓ**		
És necessari incloure la seguretat de la informació també en el desenvolupament, gestió i manteniment de l'ERP corporatiu. Es proposa dur a terme accions de formació específiques per a les persones encarregades de desenvolupar aquesta eina per tal de que es formen en mètodes i metodologies de programació segura i assoleixen la importància de generar una documentació acurada i actualitzada com a suport del treball diari.			Responsable de Programari		
OBSERVACIONS					

Observacions

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_01_051216			**DATA OB**	30/11/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.7.2.2	**ÀMBIT**	Educació, formació i conscienciació en seguretat de la informació
ENTREVISTAT			Comercial i Responsable Seguretat		
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
S'ha desenvolupat i implantat un Pla de Formació i Conscienciació en matèria de Seguretat de la informació per als treballadors però en l'últim any no s'han realitzat les accions formatives mínimes. Els treballadors del Departament de Comercial no han rebut cap sessió formativa.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Pla de Formació Continua en Seguretat de la Informació i Registres de les accions realitzades					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_02_051216			**DATA OB**	30/11/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.8.1.1	**ÀMBIT**	Inventari d'actius
ENTREVISTAT					
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
S'ha identificat alguns actius que no es troben en la última versió de l'inventari corresponent.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Inventari d'actius corporatiu					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_03_051216			**DATA OB**	30/11/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.8.3.3	**ÀMBIT**	Transferència de medis físics
ENTREVISTAT			Administratiu i Director Comercial.		
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
No existeix un log dels suports extraïbles corporatius que els empleats es porten fora de les instal·lacions ni de la informació que contenen. Quan un treballador es porta fora de les oficines un suport extraïble no deixa constància en cap document sobre aquesta acció.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de Seguretat SGSI					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_04_051216			**DATA OB**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.10.1.2	**ÀMBIT**	Administració de claus
ENTREVISTAT			Tècnic		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - OBSERVACIÓ					
No es comprova la renovació periòdica de les claus utilitzades i generades en els llocs de treball.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de Xifrat de Dades i registres derivats d'aquesta					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_05_051216			**DATA OB**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.11.1.4	**ÀMBIT**	Protecció contra riscos externs i d'entorn
ENTREVISTAT			Responsable Seguretat		
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
Continua existint un únic extintor al CPD a banda dels existents a nivell d'edifici.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Avaluació in-situ del CPD i Política de Seguretat SGSI					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_06_051216			**DATA OB**	01/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.11.1.5	**ÀMBIT**	Treball en àrees segures
ENTREVISTAT			Responsable de Seguretat		
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
No existeix una política definida per a treballar en àrees segures. El CPD corporatiu i el "warm site" de backup allotgen tots els equips i infraestructures crítiques per l'empresa però no es poden catalogar com àrees segures estrictament. Per aquest motiu, es considera oportú notar aquest aspecte únicament com observació.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Política de Seguretat SGSI					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_07_051216			**DATA OB**	02/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.11.2.3	**ÀMBIT**	Seguretat del cablejat
ENTREVISTAT			Responsable Tècnic		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - OBSERVACIÓ					
No existeix un procediment estandarditzat sobre seguretat en el cablejat corporatiu. No obstant això per la ubicació de les oficines de l'empresa i la seguretat física disponible a nivell d'edifici no es considera un aspecte crític. Per aquest motiu, es considera oportú notar aquest aspecte únicament com observació.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_08_051216			**DATA OB**	02/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.13.1.2	**ÀMBIT**	Seguretat en serveis de xarxa
ENTREVISTAT			Tècnic		
ÀREA			Departament d'Infraestructures		
DESCRIPCIÓ - OBSERVACIÓ					
No es supervisen o monitoren, ni tampoc es comprova que els serveis a nivell de xarxa corporativa contractats a tercers es realitzen de manera segura.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Falta de documentació generada com a conseqüència de la supervisió o comprovació					

OBSERVACIONS D'AUDITORIA					
CODI OB	OB_09_051216			**DATA OB**	02/12/2016
NORMATIVA	ISO 27002:2013	**CONTROL**	A.17.1.3	**ÀMBIT**	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació
ENTREVISTAT			Responsable de Seguretat		
ÀREA					
DESCRIPCIÓ - OBSERVACIÓ					
S'han desenvolupat els processos de revisió, verificació i avaluació de la continuïtat del negoci des del punt de vista de la seguretat de la informació encara que no es troben controls per avaluar la seua aplicació. S'ha de tenir en compte que el Pla de Continuïtat s'acaba d'implantar i està en procés de millora continua per aquest motiu aquest aspecte es fa constar únicament com a observació.					
REGISTRES I DOCUMENTACIÓ ANALITZADA					
Pla de Continuïtat					

11. Annex C: Resum Executiu

Aquest projecte es desenvolupa com a Treball Final de Màster, dintre del marc dels estudis del Màster Inter-universitari en Seguretat de les Tecnologies de la Informació i la Comunicació.

L'objectiu d'aquest projecte és aplicar els coneixements assolits durant el màster per a establir les bases a l'hora de realitzar un Pla Director de Seguretat i implantar un Sistema de Gestió de la Seguretat de la Informació en l'Empresa X.

La implantació d'un SGSI permet gestionar la seguretat de la informació de l'Empresa X mitjançant un procés sistemàtic, documentat i conegut per tota l'organització. Aquesta seguretat de la informació consisteix en la preservació de la seua confidencialitat, integritat i disponibilitat, així com dels sistemes implicats en el seu tractament.

Els estàndards en els que s'ha basat el desenvolupament del SGSI són el ISO/IEC27001:2013 i el ISO/IEC27002:13.

La implantació del SGSI s'ha dut a terme seguint el mètode del cicle PDCA o cicle de Deming, inclòs i descrit en l'estàndard ISO27000. Aquest mètode es basa en procés iteratiu de qualitat en quatre fases: Plan - Do - Check - Act. Mitjançant l'aplicació d'aquest mètode s'aconsegueix crear un SGSI dins un procés o cicle de millora continua.

L'Empresa X és una empresa real, excepte pel nom. Aquesta organització proporciona serveis i solucions informàtiques i de telecomunicacions, emmarcats dins el sector de les TIC.

Les motivacions i objectius principals de l'Empresa X a l'hora d'implantar aquest SGSI són millorar l'estat de Seguretat de la Informació a nivell corporatiu i establir un procés de millora continua d'aquest, aconseguint un punt diferenciador quant a la resta d'empreses del sector davant els seus clients.

Aquest projecte s'ha desenvolupat en 5 fases:

En la primera fase, s'ha avaluat la situació actual de l'Empresa X quant a seguretat de la informació mitjançant una anàlisi GAP, i s'han identificat els actius i processos crítics de l'organització.

En la segona fase, s'ha desenvolupat el sistema de gestió documental que proporciona les bases per a la implantació del SGSI i que inclou la declaració d'aplicabilitat o SOA.

En la tercera fase, s'ha realitzat l'anàlisi de riscos que poden afectar als actius de l'empresa i s'han establert els controls necessaris perquè el risc residual quedi per baix del llindar acceptable de risc per l'organització.

Un cop arribats a la quarta fase, s'ha fet una proposta de projectes per millorar l'estat de Seguretat de la Informació i mitigar els principals riscos detectats en la fase anterior.

En la cinquena fase, s'ha valorat i avaluat la maduresa dels controls aplicats per millorar la seguretat de la informació de l'Empresa X i s'ha determinat el nivell de compliment del SGSI implantat amb la norma ISO/IEC27002:2013.

Com a conclusions finals, després de la implantació del SGSI i l'avaluació dels resultats estrets de totes les fases anteriors, es considera que mitjançant el desenvolupament i implantació d'aquest SGSI, l'Empresa X ha aconseguit millorar substancialment el seu nivell de Seguretat. A més, mitjançant posteriors cicles de millora, manteniment i actualització, aquest SGSI pot ser proposat per a una auditoria de certificació oficial sota l'estàndard ISO/IEC 27001:2013.

12. Annex D: Documentació Addicional

Arxius addicionals a la memòria dels projecte:

Nom arxiu	Descripció
BorregoRodriguez_GAP 27002_2013_TFM_Fase1.xlsx	Anàlisi diferencial o GAP de l'estat inicial de la seguretat de la informació de l'Empresa X, basat en la ISO27002:2013
BorregoRodriguezPatricia_SOA 27002_2013_TFM_Fase2.xlsx	Declaració d'Aplicabilitat de l'Empresa X, detallant els controls establerts, aplicabilitat i estat
BorregoRodriguezPatricia_Gestió Indicadors_27002_2013.xlsx	Definició dels indicadors a aplicar i la seua sistemàtica de mesura, per a mesurar l'eficàcia dels controls implantats en l'Empresa X
BorregoRodriguezPatricia_Avaluació Riscos_Fase 3.xlsx	Identificació d'actius i Anàlisi de riscos de l'Empresa X
BorregoRodriguezPatricia_AudCompliment_TFM_Fase5.xlsx	Auditoria de Compliment basada en la norma ISO27002:2013 avaluant el nivell de compliment i seguretat de la informació final de l'Empresa X
Presentació PowerPoint	Presentació del projecte a la Direcció de l'Empresa X
Defensa_projecte.mp4	Defensa del projecte