Projecte Gestió i Auditoria de la Seguretat 2015-2016

Projecte Final de Postgrau, Elaboració d'un Pla de Seguretat de la Informació

Estudiant: Francesc Lucio Subirachs

Programa: Projecte Final de Postgrau en Seguretat en serveis i aplicacions (PGAS)

Àrea: Sistemes de Gestió de la Seguretat de la Informació

Consultor: Arsenio Tortajada Gallego

Professor responsable de l'assignatura: Carles Garrigues Olivella

Centre: Universitat Oberta de Catalunya

Lliurament: 06/06/2016

FITXA DEL TREBALL FINAL

Títol del treball:	*Elaboració d'un Pla de Seguretat de la Informació*
Nom de l'autor:	*Francesc Lucio Subirachs*
Nom del consultor:	*Arsenio Tortajada Gallego*
Data de lliurament :	*06/06/16*
Àrea del Treball Final:	**Gestió i Auditoria de la Seguretat**
Titulació:	Projecte Final de Postgrau en Seguretat en serveis i aplicacions
Àrea del Treball Final:	Sistemes de Gestió de la Seguretat de la Informació
Idioma del treball:	Català
Paraules clau	Màxim 3 paraules clau, validades pel director del treball (donades els estudiants o en base a llistats, tesaurus, etc.)

Resum del Treball

Aquest treball te com a finalitat realitzar un anàlisi de la implementació d'un Sistema Gestor de la Seguretat de la Informació en una empresa amb característiques i dades basades en un entorn real, per tal d'aconseguir avaluar, millorar i planificar la revisió i l'estat de la seguretat segons la norma certificable ISO/IEC 27001 i el codi de bones pràctiques definit per la norma ISO/IEC 27002:2013.

Per a la posada en marxa i anàlisi de l'empresa s'ha recavat informació sobre la mateixa (sense especificar al 100% es dades reals ni el nom d'aquesta) i s'han seguit les directrius i metodologies descrites per la norma per a analitzar l'estat de la seguretat del seu sistema de gestió de la seguretat.

A més, s'ha dut a terme una planificació i esbossat de projectes per a optimitzar la seguretat dels actius de l'empresa basats en els riscos detectats en l'anàlisi de riscos de l'empresa.

S'ha pogut determinar i avaluar l'empresa, comparant l'estat inicial d'aquesta i el posterior als projectes per a determinar, en base als objectius inicials d'aquesta i el grau de compliment desitjat de la norma, que l'empresa ha vist incrementat el seu grau de compliment de les bones pràctiques descrites per la norma, arribant a doblar el seu grau de seguretat en el seu SGSI (segons la norma).

Abstract

This project presents an analysis of the implementation of a Safety Management System Information in a company with features and data based on a real environment, to assess, review and improve the state of security system using the guidelines for certifiable standard ISO / IEC 27001 and the code of good practices defined by ISO / IEC 27002: 2013.

For the implementation and analysis of the company has been gathered about this (without specifying the actual data is 100% or the name of it) and have followed the guidelines and methodologies described by the norm for analyze the security status of their information security management system. In addition, compliance with the standard has been improved planning security projects.

In conclusion, We want to determine company's benefit by increasing the degree of compliance for the good practice according with the ISO standards.

Tabla de contenido

1. Introducció

Aquest Treball de final de màster, que sintetitza els coneixements adquirits al llarg del pla docent del postgrau, esta especialitzat en Sistemes de Gestió de la Seguretat (d'ara en endavant SGSI). Aquest projecte, per tant, persegueix analitzar el SGSI d'una empresa, fictícia basada en una empresa real, en conseqüència de la norma ISO/IEC 27001 i la norma ISO/IEC 27002:2013 que defineix directrius, guies i bones pràctiques per a la millora de la seguretat de la informació en empreses, analitzant el compliment i els nivells de risc als que esta exposada l'organització, els seus actius i el seu personal.

2. Objectius

Amb el desenvolupament d'aquest projecte es persegueixen els següents objectius, pel que fa a competències:

- Establir les bases per a la realització del Pla Director d'una empresa.
- Analitzar la seguretat d'un sistema.
- Capacitat de l'empresa per a poder exercir la seva activitat en l'entorn de les TIC en base a un codi ètic i uns estàndards internacionalment reconeguts.
- Desenvolupar la capacitat de comunicació a públic especialitzat i no especialitzat.
- Aprenentatge autònom
- Aplicar, integrar i desenvolupar els coneixements tècnics i científics adequats per a resoldre problemes en entorns nous.

Per tant, si ens referim als objectius del contingut d'aquest projecte, es desenvoluparan les següents fases:

- Documentació normativa sobre les millors pràctiques en seguretat de la informació.
- Definició clara de la situació actual i dels objectius del SGSI.
- Anàlisi de riscos.
- Identificació i valoració dels actius corporatius com a punt de partida a un anàlisi de riscos.
- Identificació d'amenaces, avaluació i classificació d'aquestes.
- Avaluació del nivell de compliment de la ISO/IEC 27002:2013 en una organització.
- Propostes de projectes de cara a millorar la gestió de la seguretat òptima.
- Esquema Documental.

Les fases anteriorment citades, i aquest treball, es desenvoluparan en la presentació dels següents productes:

- Informe d'anàlisi diferencial
- Esquema documental ISO/IEC 27001
- Anàlisi de riscos
- Pla de projectes
- Auditoria de Compliment
- Presentació de resultats

3. La norma ISO i els Sistemes Gestors de la Seguretat de la Informació

3.1 Les normes ISO

A mesura que la seguretat s'ha consolidat com a part important dels sistemes de la informació, també ho ha anat fent la metodologia i les "bones pràctiques" sobre seguretat de la informació. Es per això que s'ha decidit emprar i fer referència a la norma ISO/IEC 27002:2013 en aquesta part prèvia al desenvolupament del projecte.

La norma ISO/IEC27002:2013 "*Information technology - Security techniques - Code of practice for information security management"* (anteriorment anomenada ISO 17799, publicat per primer cop al 1995) es la versió més recent d'un estàndard per a la seguretat de la informació publicat per l'Organització Internacional de Normalització i la Comissió Electrotècnica Internacional. A nivell de l'estat espanyol la norma es descriu amb l'equivalent UNE 71501.

Aquest estàndard proporciona recomanacions de les millors pràctiques en al gestió de la seguretat de la informació a tots els interessats i responsables en iniciar, implantar o mantenir sistemes de gestió de la seguretat de la informació, definida en l'estàndard com "la preservació de la confidencialitat, integritat i disponibilitat de la informació". Aquest recull i descriu 14 dominis principals, enfocats a diferents aspectes de l'organització i de la seguretat del sistema:

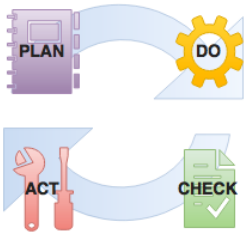
1. Polítiques de seguretat.
2. Organització de la seguretat de la informació.
3. Seguretat dels recursos humans.
4. Gestió dels actius.
5. Control d'accés.

6. Xifratge.
7. Seguretat física i ambiental.
8. Seguretat operacional.
9. Seguretat en les comunicacions.
10. Adquisició, desenvolupament i manteniment de sistemes.
11. Relacions amb els proveïdors.
12. Gestió d'incidències que afecten a la seguretat de la informació.
13. Aspectes de seguretat de la informació per a la gestió de la continuïtat del negocio.
14. Conformitat amb requisits legals i contractuals.

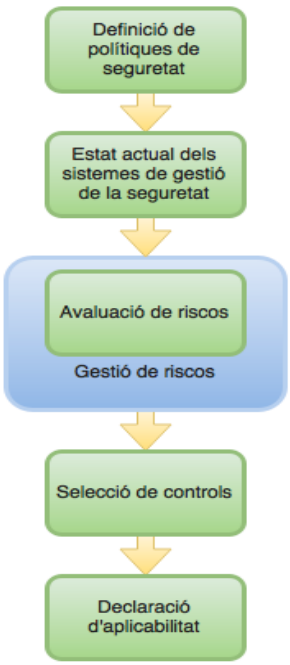
Tot i que aquest codi de bones pràctiques no es certificable la norma ISO/IEC 27001:2005 "Security techniques - Information security management systems - Requirements" si que ho es i especifica els requisits necessaris per a establir, implantar, mantenir i millorar un sistema de gestió de la seguretat de la Informació segons el procediment PDCA (plan, do, check, act). Aquesta norma es basa en les bones pràctiques descrites, permetent una certificació i anàlisi d'auditoria del compliment de la norma per part de tercers.

3.2 Els Sistemes Gestors de la Seguretat de la Informació

Un sistema de gestió de la seguretat de la informació o SGSI consisteix en un conjunt de polítiques d'administració de la informació (descrit en la norma ISO/IEC 27001). Per a una organització, disposar d'un SGSI definit és tenir dissenyar, mantenir i implantar un seguit de processos per a gestionar de manera eficient l'accessibilitat de la informació, concretament la confidencialitat, integritat i disponibilitat d'aquesta, centrant-se en aquells actius que puguin ser més rellevants per aquesta finalitat. No només es centra en els actius purament informatius si no en tots aquells actius, recursos i instal·lacions que de forma directa o indirecta puguin afectar a la informació i el desenvolupament del negoci de l'empresa. Per tant, i segons la norma descrita anteriorment, el SGSI es basa en el següent esquema per a la continua millora i optimització de la seguretat (PDCA):



Tota implantació d'un SGSI es caracteritza per organitzar-se en diferents fases, les quals venen il·lustrades pel següent diagrama:



4. Descripció de la organització (contextualització)

4.1 Missió i Història

Empresa X S.L, es una empresa que desenvolupa la seva activitat en el marc de l'educació, l'oci i la cultura, sent per tant prioritaris els serveis i productes educatius i culturals, amb una responsabilitat social i sent líders en dinamització i innovació com a base de la empresa X.

L'empresa neix als anys 70 amb l'objectiu de cobrir la demanda de material al sector cultural/educatiu amb les millors condicions de qualitat i preu. Actualment persegueix el mateix objectiu però amb la innovació i adaptació a les noves tecnologies i amb consciència social.

4.2 Descripció de l'empresa

L'empresa X es una companyia amb les següents característiques generals:

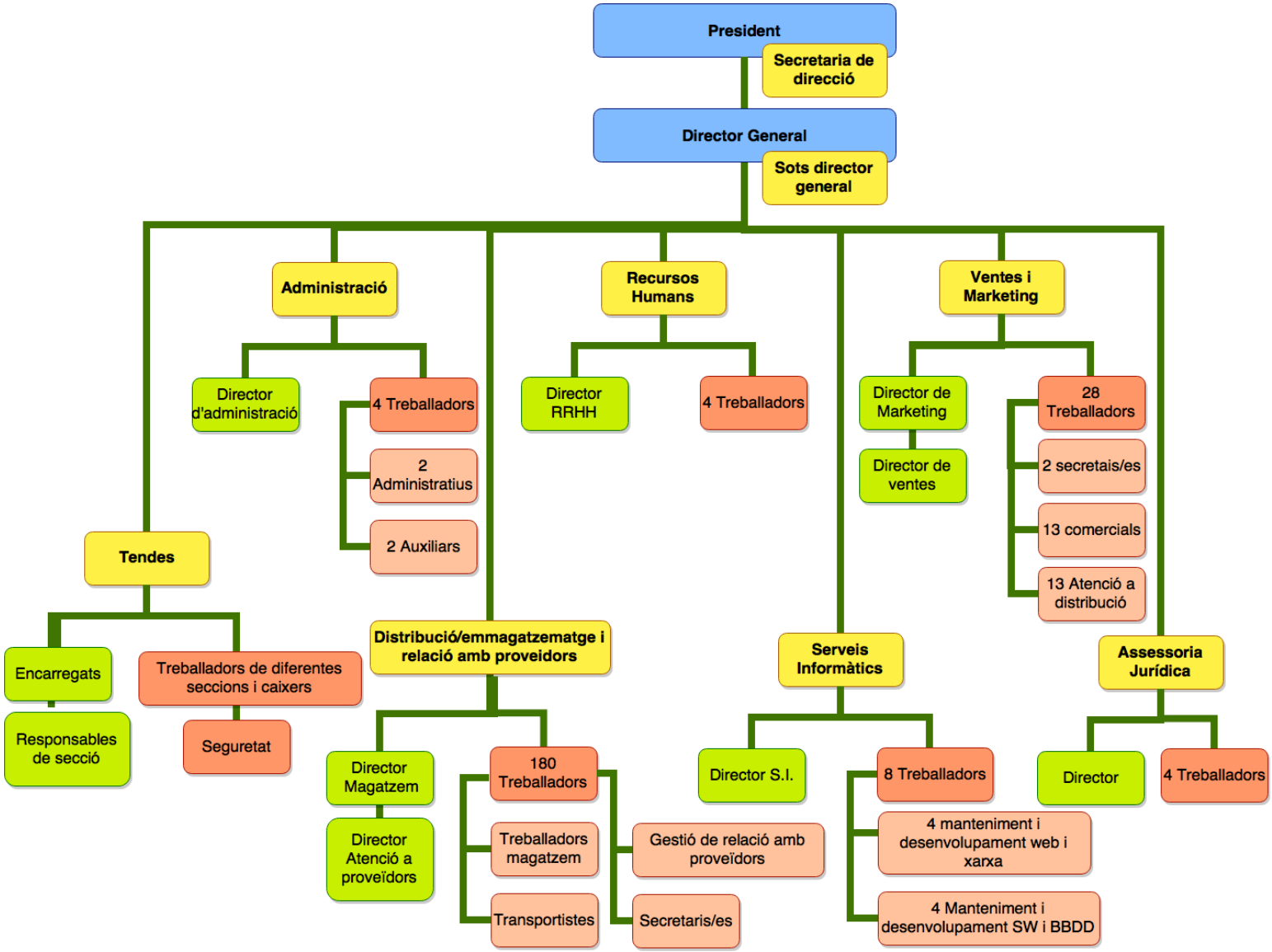
- Disposa d'una seu a Barcelona (SSCC).
- Disposa d'una amplia xarxa de 39 tendes en tot el territori de Catalunya, València i Balears.
- Disposa d'un centre logístic on es duen a terme les tasques d'embalatge, recepció de proveïdors i gestió de l'estoc dels diferents establiments.
- Disposa d'un centre de servidors per on transcorre el flux de dades de l'empresa .
- Els seus clients són particulars, empreses, escoles i associacions.
- Actualment abasteix als seus clients a través de les seves tendes (on-line i físiques) i a través de la seva xarxa de comercials i distribució en l'àmbit de les escoles, empreses o associacions.
- Te una plantilla de més de 479 empleats indefinits, i altres tants com a temporers i altres serveis associats (com per exemple seguretat de les instal·lacions, distribució, etc).
- La xarxa de centres de venta compren 31487m2 de superfície de venta.
- Genera un total de 82.265.639€ en productes distribuïts i organitza i participa en mes de 1.030 activitats culturals i socials per a públics de totes les edats.
- Te una afluència de clients de 796.160 socis i sòcies.
- Distribueix productes tecnològics, educatius/culturals i escolars.
- Els seus principals distribuïdors estan en el territori català, conformant u 65,1%, un 33,4% de a resta de l'estat espanyol i només un 1,5% procedeix de mercats estrangers.
- Forta convicció i orientació de producte social, ambiental, funcional, educatiu i tecnològic.
- També esta present en 4 empreses participades.
- Disposa d'una flota de camions de distribució i de vehicles comercials per a la realització de la distribució i desplaçament als clients (no particulars en tenda).

L'empresa X te unes projeccions de futur orientades als següents punts, però sempre mantenint els seus socis i clients en el centre del seu pla de negoci:

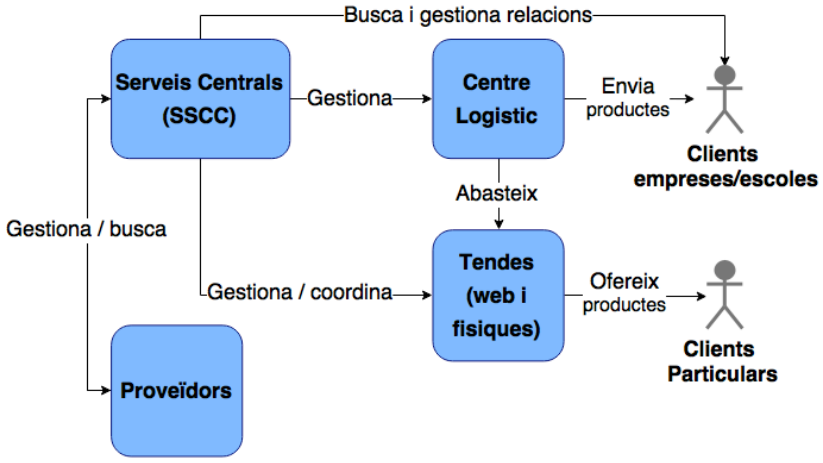
1. Mobilitat: Potenciar l'e-commerce en el seu sector i l'optimització de la web responsiva i entrar amb força en el marc de les Apps.
2. Comunicació: Integrar el client per tots els medis de comunicació actuals.
3. Omnicanalitat: Connectar i interaccionar amb tots els canals que els clients tenen disponibles.

4.3 Estructura jeràrquica i departaments

En el següent diagrama es veuen els departaments i responsables que conformen l'empresa X.

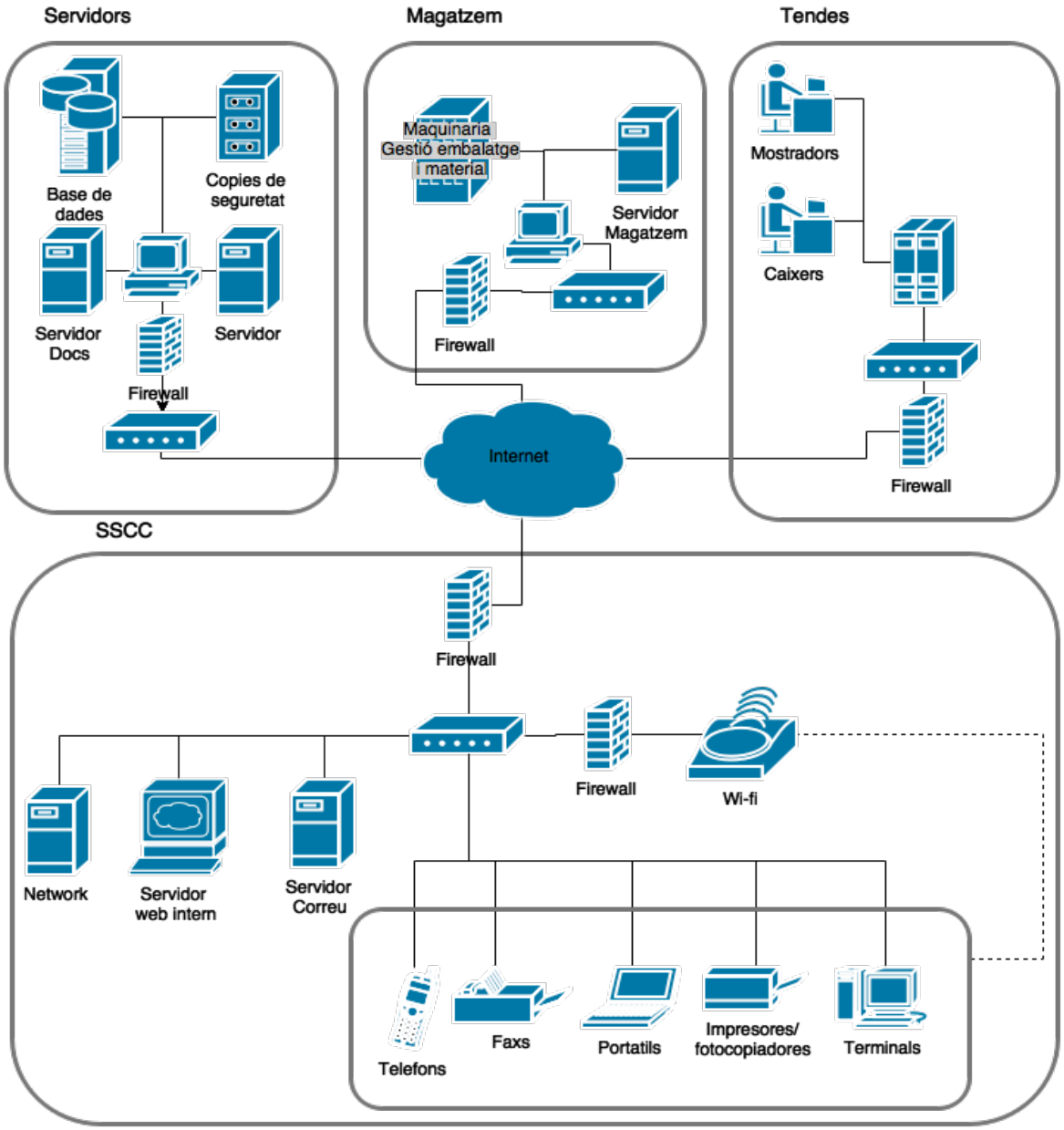


En el següent diagrama es poden observar les relacions entre dels diferents centres (SSCC, tendes, magatzem) i els clients de l'empresa.



4.4 Diagrama de xarxa

Tots els equips instal·lats en el sistema (tant a tendes, SSCC com a la resta d'instal·lacions es basen en Windows 7 amb actualitzacions periòdiques de Windows up-date server (privat), amb les llicències ne regla i actualitzades. Tot el desenvolupament de les tasques dels departaments dels sscc es basa en un sistema SAP i els terminals de les tendes es comuniquen directament amb un servidor (de la tenda) que envia informació de negoci als servidors de sscc.



Els telèfons corporatius son Windows phone connectats a la xarxa de SSCC mitjançant wi-fi o 3G a l'exterior, podent actuar així com a routers per als portàtils si els comercials ho necessiten.

4.5 Estat de la seguretat de l'empresa

L'empresa disposa de diferents mesures, protocols o mecanismes en funció del centre. En els seus serveis centrals disposa de mecanismes de vídeo-vigilància 24h en tot el perímetre i zones comuns interiors, alarmes, vigilant de recepció, verificació i fitxatge de tots els treballadors i/o visitants que puguin accedir a l'edifici mitjançant targetes d'identificació enregistrades en una base de dades de personal autoritzat, gestionat únicament per RRHH amb autorització del director d'aquest departament i, per altra banda, disposen de mecanismes preventius contra incendis mitjançant l'aïllament de la zona d'accés a l'arxiu i servidors (amb sistema d'extracció de l'oxigen per a apagar el foc).

A més en els SSCC també hi disposen de encriptació dels ordinadors i arxius emmagatzemats en aquests amb contrasenya personal de cada treballador, la qual, només pot ser assignada i modificada per RRHH en consonància amb el departament d'informàtica. Pel que fa a les dades que es gestionen, aquestes estan emmagatzemades en un servidor en un centre extern, aquestes dades es gestionen mitjançant diverses plataformes software (entre elles plataforma SAP) i, a més, se'n realitzen copies de recuperació programades per assegurar l'accés a les dades.

Les dades emmagatzemades en els servidors estan protegides per un sistema de claus d'accés (les de cada empleat i en funció del nivell de càrrec que es tingui es pot accedir o gestionar de maneres diferents i a continguts diferents); a més pel que fa al centre on estan els servidors, aquests estan protegits amb sistemes contra incendis, talls elèctrics i inundacions.

Pel que fa al serveis logístics d'emmagatzematge, les mesures de seguretat son iguals que en el SSCC però amb la diferència que s'ha de comptar amb la zona d'aparcament dels camions de distribució i majors mesures contra danys climatològics. Les dades que s'hi tracten i els equips que s'utilitzen segueixen la mateixa configuració que els situats en els serveis centrals.

Per altra banda, pel que fa als establiments, es disposen de mecanismes típics propis d'una tenda, tals com: alarma i vídeo-vigilància del back-office i del front-office, arcs de detecció d'alarmes, caixes enregistradores amb apertura automàtica i amb accés restringit als empleats autoritzats, caixa forta, accés a l'obertura de l'establiment mitjançant claus de seguretat físiques i claus de N dígits per a desconnexió dels sistemes de seguretat que només estiguin actius fora d'horari al públic; a més compten amb personal de seguretat per a gestionar incidents puntuals i equips amb accés per contrasenya similars als situats en els serveis centrals.

També cal comentar que totes les claus de pas lògiques, com les contrasenyes de les sessions dels treballadors, caduquen de forma automatitzada al cap de 6 mesos, tenint que canviar aquestes per una diferent cada cop sense repetir cap de les dues contrasenyes anteriors.

4.6 Protocol de copies de seguretat

Les copies de seguretat de les dades i fitxers de l'empresa es realitzen de forma automàtica diària els canvis realitzats sobre la copia del dia anterior i així successivament eliminant així copies innecessàries i conservant un exemplar de copia mensual per si es tingues que realitzar un back-up sobre aquesta.

Les copies s'emmagatzemen en format cinta i es realitzen en un servidor dedicat en centre de servidors de l'empresa.

4.7 Objectius

L'empresa X pretén assolir, al llarg dels pròxim any, els següents ítems:

1. Millorar la connectivitat i relació dels clients.
2. Nodrir la dimensió social de l'empresa i mantenir unes condicions mediambientals sostenibles.
3. Millorar i optimitzar els seus serveis web i mòbils.
4. Mantenir una qualitat de preu i servei en els materials que ven.
5. Protegir la informació dels seus clients i proveïdors

6. Protegir els articles que distribueix
7. Donar seguretat en les transaccions i serveis virtuals als seus clients
8. Optimitzar la seguretat en les oficines i tendes
9. Minimitzar la fuga d'informació personal i corporativa
10. Minimitzar la complexitat de la gestió de les dades dels clients i proveïdors, maximitzant la seguretat d'aquestes dades.
11. Minimitzar les pèrdues econòmiques per la sostracció de materials de venta
12. Maximitzar la seguretat dels diners que es gestionen a les tendes.
13. Mantenir seguretat i fiabilitat transaccional amb les targetes financeres dels clients.
14. Millorar la seguretat i la coordinació de les comandes a clients i a botigues.
15. Maximitzar la seguretat laboral.
16. Implementar sistemes de protecció contra amenaces SW externes i internes per millorar les ja existents.
17. Augmentar la seguretat en les relacions amb els proveïdors; tant en la informació com en les mercaderies.
18. Compliment dels requisits i marcs legals actuals (actualització, en cas de ser necessària, segons la normativa vigent).

Partint dels objectius plantejats per al futur definits podem afirmar que el pla director de seguretat abasteix la millora i el perfeccionament dels mecanismes i sistemes de seguretat que protegeixen els actius i els treballadors de l'empresa a més de mantenir el seu compromís social i ambiental durant tot aquest procés de millora.

4.8 Anàlisis diferencial

A continuació es poden observar els nivells de Maduresa dels diferents sub-apartats definits per la norma ISO/IEC 27002, amb els que se n'extreu el nivell de compliment de cada apartat definit en aquesta norma; considerant així el percentatge obtingut com a tal.

5.POLÍTICA DE SEGURETAT.	30,00%
5.1 Política de seguretat de la informació.	30,00%
5.1.1 Document de política de seguretat de la informació.	20,00%
5.1.2 Revisió de la política de seguretat de la informació.	40,00%
6-ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	46,07%
6.1 Organització interna.	42,14%
6.1.1 Compromís de la Direcció amb la seguretat de la informació.	90,00%
6.1.2 Coordinació de la seguretat de la informació.	25,00%
6.1.3 Assignació de responsabilitats relatives a la seg. de la informac.	10,00%
6.1.4 Procés d'autorització de recursos per al tractament de la informació.	10,00%
6.1.5 Acords de confidencialitat.	70,00%
6.1.6 Contacte amb les autoritats.	80,00%
6.1.7 Contacte amb grups d'especial interès.	10,00%
6.1.8 Revisió independent de la seguretat de la informació.	10,00%
6.2 Tercers.	50,00%
6.2.1 Identificació dels riscos derivats de l'accés de tercers.	10,00%
6.2.2 Tractament de la seguretat en la relació amb els clients.	95,00%
6.2.3 Tractament de la seguretat en contractes amb tercers.	45,00%
7.Gestió D'ACTIUS.	72,50%
7.1 Responsabilitat sobre els actius.	85,00%
7.1.1 Inventari d'actius.	95,00%
7.1.2 Propietat dels actius.	90,00%
7.1.3 Ús acceptable dels actius.	70,00%

7.2 Classificació de la informació.	60,00%
7.2.1 Directrius de classificació.	50,00%
7.2.2 Etiquetatge i manipulat de la informació.	70,00%
8.SEGURIDAD LLIGADA ALS RECURSOS HUMANS.	36,11%
8.1 Abans de l'ocupació.	30,00%
8.1.1 Funcions i responsabilitats.	40,00%
8.1.2 Investigació d'antecedents.	20,00%
8.1.3 Condicions de contractació.	30,00%
8.2 Durant l'ocupació.	65,00%
8.2.1 Responsabilitats de la Direcció.	70,00%
8.2.2 Conscienciació, formació i capacitació en seg. de la informac.	55,00%
8.2.3 Procés disciplinari.	70,00%
8.3 Cessament de l'ocupació o canvi de lloc de treball.	13,33%
8.3.1 Responsabilitat del cessament o canvi.	10,00%
8.3.2 Devolució d'actius.	10,00%
8.3.3 Retirada dels drets d'accés.	20,00%
9.SEGURIDAD FÍSICA I DE L'ENTORN.	53,81%
9.1 Àrees segures.	68,33%
9.1.1 Perímetre de seguretat física.	60,00%
9.1.2 Controls físics d'entrada.	95,00%
9.1.3 Seguretat d'oficines, despatxos i instal·lacions.	95,00%
9.1.4 Protecció contra les amenaces externes i d'origen ambiental.	90,00%
9.1.5 Treball en àrees segures.	30,00%
9.1.6 Àrees d'accés públic i de càrrega i descàrrega.	40,00%
9.2 Seguretat dels equips.	39,29%
9.2.1 Emplaçament i protecció d'equips	60,00%
9.2.2 Instal·lacions de subministrament.	15,00%
9.2.3 Seguretat del cablejat.	40,00%
9.2.4 Manteniment dels equips.	40,00%
9.2.5 Seguretat dels equips fora de les instal·lacions.	40,00%
9.2.6 Reutilització o retirada segura d'equips.	40,00%
9.2.7 Retirada de materials propietat de l'empresa.	40,00%

10.GESTIÓN DE COMUNICACIONS I OPERACIONS.	66,88%
10.1 Responsabilitats i procediments d'operació.	61,25%
10.1.1 Documentació dels procediments d'operació.	70,00%
10.1.2 Gestió de canvis.	65,00%
10.1.3 Segregació de tasques.	70,00%
10.1.4 Separació dels recursos de desenvolupament, prova i operació.	40,00%
10.2 Gestió de la provisió de serveis per tercers.	90,00%
10.2.1 Provisió de serveis.	90,00%
10.2.2 Supervisió i revisió dels serveis prestats per tercers.	90,00%
10.2.3 Gestió del canvi en els serveis prestats per tercers.	90,00%
10.3 Planificació i acceptació del sistema.	77,50%
10.3.1 Gestió de capacitats.	80,00%
10.3.2 Acceptació del sistema.	75,00%
10.4 Protecció contra el codi maliciós i descarregable.	50,00%
10.4.1 Controls contra el codi maliciós.	50,00%
10.4.2 Controls contra el codi descarregat al client.	50,00%
10.5 Còpies de seguretat.	95,00%
10.5.1 Còpies de seguretat de la informació.	95,00%
10.6 Gestió de la seguretat de les xarxes.	72,50%
10.6.1 Controls de xarxa.	65,00%
10.6.2 Seguretat dels serveis de xarxa.	80,00%
10.7 Manipulació dels suports.	40,00%
10.7.1 Gestió de suports extraïbles.	10,00%
10.7.2 Retirada de suports.	10,00%
10.7.3 Procediments de manipulació de la informació.	70,00%
10.7.4 Seguretat de la documentació del sistema.	70,00%
10.8 Intercanvi d'informació.	50,00%
10.8.1 Polítiques i procediments d'intercanvi d'informació.	50,00%
10.8.2 Acords d'intercanvi.	50,00%
10.8.3 Suports físics en trànsit.	50,00%
10.8.4 Missatgeria electrònica.	50,00%

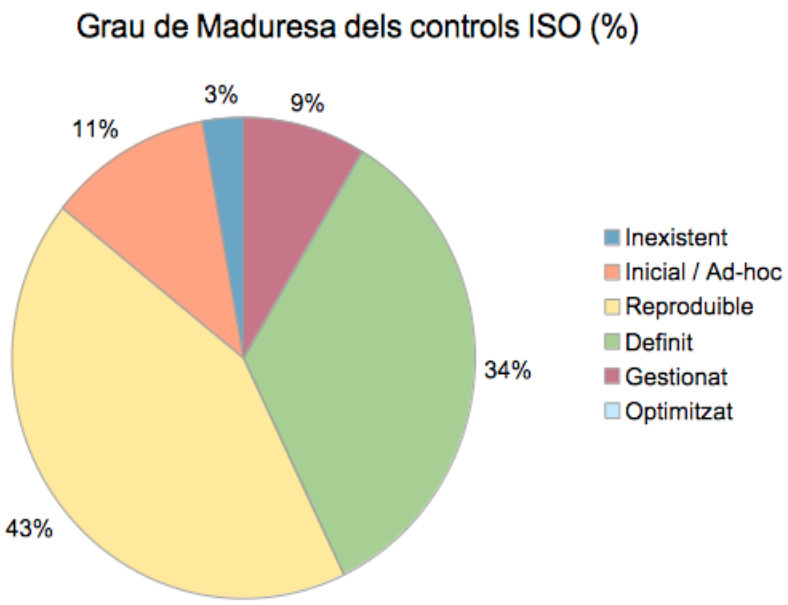
10.8.5 Sistemes d'informació empresarials.	50,00%
10.9 Serveis de comerç electrònic.	96,67%
10.9.1 Comerç electrònic.	95,00%
10.9.2 Transaccions en línia.	95,00%
10.9.3 Informació públicament disponible.	100,00%
10.10 Supervisió.	35,83%
10.10.1 Registres d'auditoria.	10,00%
10.10.2 Supervisió de l'ús del sistema.	15,00%
10.10.3 Protecció de la informació dels registres.	50,00%
10.10.4 Registres d'administració i operació.	50,00%
10.10.5 Registre de fallades.	40,00%
10.10.6 Sincronització del rellotge.	50,00%
11.11.CONTROL D'ACCÉS.	61,11%
11.1 Requisits de negoci per al control d'accés.	40,00%
11.1.1 Política de control d'accés.	40,00%
11.2 Gestió d'accés d'usuari.	93,75%
11.2.1 Registre d'usuari.	95,00%
11.2.2 Gestió de privilegis.	95,00%
11.2.3 Gestió de contrasenyes d'usuari.	95,00%
11.2.4 Revisió dels drets d'accés d'usuari.	90,00%
11.3 Responsabilitats d'usuari.	90,00%
11.3.1 Ús de contrasenyes.	90,00%
11.3.2 Equip d'usuari desatès.	90,00%
11.3.3 Política de lloc de treball buidat i pantalla neta.	90,00%
11.4 Control d'accés a la xarxa.	75,71%
11.4.1 Política d'ús dels serveis en xarxa.	95,00%
11.4.2 Autenticació d'usuari per a connexions externes.	40,00%
11.4.3 Identificació dels equips en les xarxes.	95,00%
11.4.4 Protecció dels ports de diagnòstic i configuració remots.	80,00%
11.4.5 Segregació de les xarxes.	80,00%
11.4.6 Control de la connexió a la xarxa.	60,00%
11.4.7 Control d'encaminament (routing) de xarxa.	80,00%
11.5 Control d'accés al sistema operatiu.	53,33%

11.5.1 Procediments segurs d'inici de sessió.	70,00%
11.5.2 Identificació i autenticació d'usuari.	90,00%
11.5.3 Sistema de gestió de contrasenyes	90,00%
11.5.4 Ús dels recursos del sistema.	70,00%
11.5.5 Desconnexió automàtica de sessió.	0,00%
11.5.6 Limitació del temps de connexió.	0,00%
11.6 Control d'accés a les aplicacions i a la informació.	65,00%
11.6.1 Restricció de l'accés a la informació.	40,00%
11.6.2 Aïllament de sistemes sensibles.	90,00%
11.7 Ordinadors portàtils i teletreball.	10,00%
11.7.1 Ordinadors portàtils i comunicacions mòbils.	10,00%
11.7.2 Teletreball.	10,00%
12.12.ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE SISTEMES D'INFORMACIÓ.	20,33%
12.1 Requisits de seguretat dels sistemes d'informació.	20,00%
12.1.1 Anàlisi i especificació dels requisits de seguretat.	20,00%
12.2 Tractament correcte de les aplicacions.	30,00%
12.2.1 Validació de les dades d'entrada.	20,00%
12.2.2 Control del processament intern.	40,00%
12.2.3 Integritat dels missatges.	20,00%
12.2.4 Validació de les dades de sortida.	40,00%
12.3 Controls criptogràfics.	0,00%
12.3.1 Política d'ús dels controls criptogràfics.	10,00%
12.3.2 Gestió de claus.	10,00%
12.4 Seguretat dels arxius de sistema.	10,00%
12.4.1 Control del programari en explotació.	10,00%
12.4.2 Protecció de les dades de prova del sistema.	10,00%
12.4.3 Control d'accés al codi font dels programes.	10,00%
12.5 Seguretat en els processos de desenvolupament i suport.	22,00%
12.5.1 Procediments de control de canvis.	10,00%

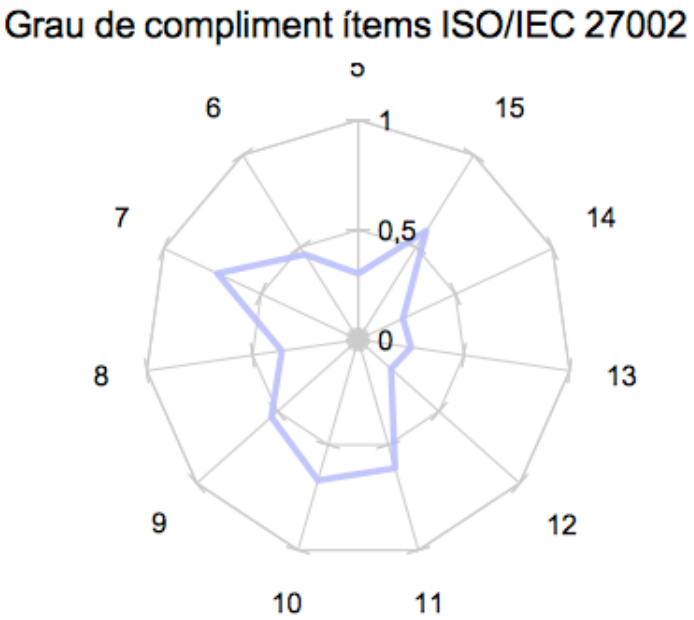
12.5.2 Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu.	10,00%
12.5.3 Restriccions als canvis en els paquets de programari.	10,00%
12.5.4 Fuites d'informació.	80,00%
12.5.5 Externalització del desenvolupament de programari.	0,00%
12.6 Gestió de la vulnerabilitat tècnica.	40,00%
12.6.1 Control de les vulnerabilitats tècniques.	40,00%
3.13.GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	25,00%
13.1 Notificació d'esdeveniments i punts febles de seguretat de la informació.	40,00%
13.1.1 Notificació dels esdeveniments de seguretat de la informació.	40,00%
13.1.2 Notificació de punts febles de seguretat.	40,00%
13.2 Gestió d'incidents i millores de seguretat de la informació.	10,00%
13.2.1 Responsabilitats i procediments.	10,00%
13.2.2 Aprenentatge dels incidents de seguretat de la informació.	10,00%
13.2.3 Recull d'evidències.	10,00%
14.GESTIÓN DE LA CONTINUÏTAT DEL NEGOCI.	23,00%
14.1 Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci.	23,00%
14.1.1 Inclusió de la seguretat de la informació en el procés de gestió de la continuïtat del negoci.	15,00%
14.1.2 Continuïtat del negoci i avaluació de riscos.	30,00%
14.1.3 Desenvolupament i implantació de plans de continuïtat que incloguin la seguretat de la informació.	30,00%
14.1.4 Marc de referència per a la planificació de la cont. del negoci.	20,00%
14.1.5 Proves, manteniment i re-avaluació de plans de continuïtat.	20,00%
15.CUMPLIMENT.	58,89%
15.1 Compliment dels requisits legals.	81,67%

15.1.1 Identificació de la legislació aplicable.	40,00%
15.1.2 Drets de propietat intel·lectual (DPI).	90,00%
15.1.3 Protecció dels documents de l'organització.	90,00%
15.1.4 Protecció de dades i privacitat de la informació de caràcter personal.	90,00%
15.1.5 Prevenció de l'ús indegut de recursos de tractament de la informació.	90,00%
15.1.6 Regulació dels controls criptogràfics.	90,00%
15.2 Compliment de les polítiques i normes de seguretat i compliment tècnic.	85,00%
15.2.1 Compliment de les polítiques i normes de seguretat.	90,00%
15.2.2 Prova de conformitat tècnic.	80,00%
15.3 Consideracions sobre les auditories dels sistem. d'informació.	10,00%
15.3.1 Controls d'auditoria dels sistemes d'informació.	10,00%
15.3.2 Protecció de les eines d'auditoria dels sist. d'informació	10,00%

Dels graus de compliment de l'empresa X avaluats n'extrèiem el següent gràfic on hi podem observar la situació general del compliment dels ítems que conformen els apartats de la norma.



En canvi, en el següent gràfic hi podem observar el grau percentual del compliment dels controls definits per la norma per a l'estat actual de la nostra empresa.



5. Sistema de Gestió documental

Tots els sistemes de gestió de la seguretat de la informació es recolzen en un cos documental per al compliment normatiu. Per aquest motiu, i segons el definit a la norma ISO/IES 27001, en aquest apartat es recullen els documents, taules i polítiques que són d'aplicació en el SGSI de la nostra empresa XXXX.

5.1 Política de Seguretat

L'empresa, així com el seu director general i els accionistes son conscients i consideren de vital importància el de que per a crear, mantenir i millorar la confiança del seus clients i distribuïdors així com per assegurar el futur i el bon funcionament de l'empresa la seguretat de la informació juga un paper clau per aconseguir-ho.

Per tant l'empresa ha desenvolupat una Política de Seguretat, definint els procediments que haurien de garantir la confidencialitat, integritat i disponibilitat de la informació necessària per a complir les seves promeses de cara a la societat, els clients i els membres que conformen l'empresa.

Es per aquests motius que l'empresa te implementat i ara vol avaluar i millorar el seu sistema de gestió de la seguretat. Això es amb la intenció d'oferir el millor servei, respectant els drets legalment establerts per a cadascuna de les parts implicades en el desenvolupament de la seva activitat.

L'abast de les polítiques de seguretat que l'empresa estableix s'estenen a tots i cadascun dels membres que formen part d'aquesta, de manera que tots aquests les han de conèixer i assumir com a part de les seves funcions laborals.

L'empresa estableix els següents principis de seguretat:

- La informació, així com els sistemes informàtics, son valors crucials i de vital importància; per tant sense protecció sobre aquesta informació el futur de l'empresa es veuria afectat. El manteniment d'un nivell de protecció de la informació és un aspecte tant important com la protecció de la resta d'actius valuosos per a l'empresa.
- L'empresa considera que la protecció de la informació i la resta d'actius passa primerament per un treball en equip, és adir, tota l'empresa s'ha d'implicar en els protocols, normes i bones pràctiques per aconseguir els objectius de seguretat que es planteja.

L'empresa estableix les responsabilitats de cadascun dels membres d'aquesta sota una normativa interna, així com els protocols per a protegir la informació davant d'amenaces tals com la destrucció, manipulació, difusió no autoritzada, reproducció, pèrdua, mal ús, apropiació, etc.

- Tots els treballadors de la companyia (sense excepció) han de complir la normativa per assegurar la protecció de la informació descrita en la política de seguretat de l'empresa. Establint així accions disciplinàries per aquells que infringeixin les normes.
- D'igual manera la normativa de seguretat s'aplica a tots els ordinadors, plataformes, sistemes i altres dispositius electrònics de l'empresa.
- L'ús dels diferents sistemes informàtics es limiten única i exclusivament a l'ús laboral i en cap cas per a finalitats personals. Així mateix esta prohibida la instal·lació de programari no autoritzat i sense conformitat dels departaments responsables en el maquinari de l'empresa.
- Es permet la utilització de suports d'emmagatzematge extern (USB, HDD, CD) per a realitzar el desenvolupament d'activitats de l'empresa o per a temes publicitaris (cedint-los, per exemple a proveïdors i col·laboradors per a l'elaboració de material).
- Tots els recursos de l'empresa, únicament es podran utilitzar amb finalitats directament vinculades amb l'activitat de l'empresa i mai amb finalitats personals.

- Únicament els dispositius propietat de l'empresa es podran connectar a la xarxa d'aquesta.
- Tots els sistemes informàtics estaran dotats de sistemes de seguretat via Software.

Tant mateix, l'empresa estableix les responsabilitats de mantenir, gestionar i garantir la seguretat de la informació sobre el departament d'informàtica, sota la supervisió de la direcció de l'empresa. S'estableixen categories per a assegurar un correcte accés a la informació en funció dels permisos que cada usuari, en relació amb el seu càrrec o rol, li pertoquen:

- Autorització de lectura: únicament poden consultar-la i visualitzar-la, seria el cas d'un caixer, el qual només pot consultar detalls i preus dels articles que ven.
- Autorització a modificació i lectura: poden consultar i afegir informació al sistema, serien per exemple encarregats de SSCC que duen a terme tasques relacionades amb productes nous o productes obsolets que s'han d'incorporar al servei dels clients o per altra banda s'han d'eliminar de l'estoc.
- Autorització total sobre la informació: estan autoritzats realitzar qualsevol acció sobre la informació, restringit únicament a la direcció dels departaments de l'empresa i a tot el departament encarregat de desenvolupar les aplicacions, infraestructures lògiques i gestió de les bases de dades de l'empresa.

L'empresa fica les responsabilitats de tots els usuaris, proveïdors, empleats i sistemes per al maneig consistent de la informació, per assegurar la legalitat del tractament d'aquesta i els drets legals de totes les parts implicades a la confidencialitat i control de la informació que els referència per part de la empresa. L'empresa assegurarà la correcta manipulació mitjançant mecanismes de seguretat, ja sigui lògics per a tota aquella dada confidencial de caràcter digital o sistemes de seguretat física per a les dades emmagatzemades en formats físics (per exemple paper).

L'administrador de sistemes es l'encarregat de gestionar els procediments i la planificació de les còpies de seguretat per tal de garantir la recuperació de la

informació vital de l'empresa en cas de fallades o catàstrofes.

L'empresa defineix controls d'accés a la informació, establint el següent:

- L'accés a la informació propietat o sota custodia de l'empresa només la podrà consultar els treballadors amb necessitat legítima de consultar-la per al desenvolupament del negoci.
- Els empleats no poden accedir a la informació confidencial sense autorització per part de la direcció i els propietaris d'aquesta. En cas de vulnerar-se aquest dret, el superior de l'empleat haurà de notificar-ho immediatament a instàncies superiors.
- Tots els empleats tenen assignat un nom d'usuari únic i una contrasenya personal, permetent així l'accés al mateix sistema informàtic però podent establir així restriccions en funció dels privilegis de cada usuari.
- Cada empleat es personalment responsable de l'ús del seu nom d'usuari i contrasenya.
- Cada empleat es responsable de l'ús i accions que fa sobre la informació de l'empresa a la qual accedeix o gestiona.
- Els usuaris anònims estaran permesos amb prèvia autorització de recursos humans, sent aquest de tipus Convidat i per tant sense cap privilegi d'accés a la informació del sistema.
- Les contrasenyes en tot cas hauran de ser difícils d'endevinar imposant contrasenyes de mes de 8 caràcters alfanumèrics que continguin al menys una lletra en majúscula i una en minúscula juntament amb com a mínim un número; questes contrasenyes tindran una caducitat per tal de minimitzar l'impacte del robatori de contrasenyes.
- Les contrasenyes no es poden emmagatzemar en cap mena de suport (ni físic ni digital) ni compartir-se amb altres persones (siguin empleats o no).

L'empresa distingeix diferents incidents de seguretat, i estableix el protocol a seguir en cadascun d'aquest incidents. En son exemples:

- Robatori amb o sense lesió del personal: en cas de robatori en els seus centres de venta, la seguretat dels empleats i els clients esta per sobra dels actius de l'empresa i la seva informació. S'avisarà a les forces de seguretat i serveis sanitaris corresponents per a que duguin a terme investigació i per a donar atenció a les víctimes i afectats, si els hi ha (públic o empleats).
- Robatori d'equips: tots els equips estaran protegits amb sistemes antirobatori (per exemple sistemes Kengsinton, en cas de ser dispositius immòbils, i en cas dels portàtils estaran degudament etiquetats i identificats per a la seva localització fora dels límits de la empresa.
- Actuació il·legítima sobre la informació: s'identificaran els empleats que han accedit a la informació i es duran a terme les investigacions necessàries (accedint als sistemes utilitzats i a la informació dels servidors que utilitza l'empleat) per a identificar l'infractor i aplicar les sancions o acomiadaments pertinents.
- En cas de destrucció o mal ús dels equips, instal·lacions o articles de venta de l'empresa, els empleats seran identificats i sancionats.
- En cas de catàstrofe de tipus ambiental-climatològica s'avaluarà els danys i s'informarà a la corresponent companyia d'assegurances.
- En tots els casos la seguretat dels empleats i els clients (en el cas dels establiments de venta) imperen per sobre de la informació, els dispositius i les instal·lacions.

Per a la supervisió, manteniment i definició de les polítiques de seguretat corresponents al SGSI implantat, l'empresa disposa d'un comitè de seguretat de la informació, el qual el conformen el cap de cada departament (RRHH, Serveis Informàtics, Gestió de proveïdors, Comercials, etc) que, juntament amb el Director general i el secretari decideixen i planifiquen els aspectes directament relacionats amb la seguretat de la informació. Aquests es reuneixen de forma periòdica i enregistren les actes (signades per tots ells de forma física) per tal de poder dur a terme les revisions i implementacions de millora necessàries sobre el SGSI.

5.2 Procediment d'auditories internes

Per a auditar el SGSI, s'estableix una planificació de les auditories que es duran a terme durant la vigència de la certificació (un cop obtinguda), on s'establiran els requisits per als auditors interns i es definirà el model de l'informe de l'auditoria. Per a poder dur a terme l'auditoria s'estableixen els següents punts:

- L'abast: revisar, avaluar i qualificar el grau de protecció dels elements actius de l'empresa que contenen informació sensible, mitjançant l'avaluació de les mesures de seguretat físiques i lògiques establertes, la correcta planificació del SGSI, la vulnerabilitat del sistema, la pèrdua d'informació i violació d'aquesta i la correcta gestió dels actius de l'empresa en relació al compliment de la norma ISO/IEC 27001. Per a fer-ho s'avaluaran:
    - Sistemes de control d'accés lògic
    - Sistemes de control d'accés físic
    - Grau de protecció dels sistemes i actius de l'empresa
    - Grau de pèrdues d'actius valuosos
    - Grau de compliment de la norma
    - Avaluació del transport i la distribució

  No s'entrarà en detalls logístics, centrant-nos en la gestió dels actius i la informació per part de SSCC i punts de venta, sense avaluar els processos mecanitzats de gestió de magatzem.

- Requisits de l'equip d'auditoria: Pel que fa a l'estructura de les persones responsables de dirigir el programa d'auditoria, fer-ne el seguiment i realitzar l'auditoria, haurien de acomplir les següents característiques i rols:
    - Coneixements tècnics de bases de dades
    - Coneixements tècnics de servidors web i servidors d'aplicació
    - Coneixements de seguretat i dimensionament de xarxes
    - Coneixements de legislació vigent en matèria de protecció de dades i drets laborals

- Habilitats de gestió
- Coneixements en sistemes criptogràfics
- Coneixements generals de principis de l'auditoria
- Coneixement de gestió de fitxers
- Coneixements de dispositius i tecnologies de seguretat física

5.3 Model de l'informe d'auditoria interna

Per a cada indicador, aspecte o criteri a auditar es seguirà el següent patró o fitxa en el que s'hi documentarà l'abast de les proves realitzades, els detalls de l'actuació auditora, els intervinents, el procés i àrea a auditar i les observacions i la presentació dels resultats.

<table>
<tr><td colspan="7">Procés o àrea a auditar:</td></tr>
<tr><td colspan="7">Objectiu de l'auditoria:</td></tr>
<tr><td colspan="7">Abast de l'auditoria:</td></tr>
<tr><td colspan="7">Criteris de l'auditoria:</td></tr>
<tr><td colspan="7">Auditors</td></tr>
<tr><td colspan="7">Nom auditor/s:</td></tr>
<tr><td colspan="2">Auditat</td><td colspan="2">Inici de l'activitat</td><td colspan="2">Tancament de l'activitat</td><td rowspan="2">AUDITOR</td></tr>
<tr><td>Activitat o criteri</td><td>Carreg del responsable del procés</td><td>Data</td><td>Hora</td><td>Data</td><td>Hora</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="7">Observacions:</td></tr>
<tr><td colspan="7">Conclusions:</td></tr>
<tr><td colspan="2">Auditor en cap:
Nom

Firma</td><td colspan="2">Auditat:
Nom

Firma</td><td colspan="3">Auditor/s:
Nom/s

Firma</td></tr>
</table>

- Pla genèric d'auditoria: seguint el document (fitxa) mostrat en el punt anterior, es planificarà un conjunt de proves que conformarà una auditoria de forma semestral de manera que es podran avaluar els diferents graus de compliment dels protocols establerts en el SGSI per tal d'avaluar-lo. Partim de la consideració que la certificació caduca als 3 anys, de manera que estaríem parlant de 6 processos d'auditoria interna per tal de revisar el SGSI.

5.4 Gestió d'indicadors

Es defineixen un seguit d'indicadors per a la gestió i compliment del model de gestió de la seguretat de la informació, són els següents:

<table>
<tr><th colspan="6">Indicador: Organització de seguretat de la informació</th></tr>
<tr><td colspan="2">Identificador</td><td colspan="4">SGSI_ID_1</td></tr>
<tr><td colspan="6">Definició</td></tr>
<tr><td colspan="6">Determina i segueix el compromís de la direcció, en àmbits de gestió de la seguretat de la informació, en l'assignació de personal i responsabilitats relacionades amb la seguretat de la informació de l'empresa</td></tr>
<tr><td colspan="6">Objectiu</td></tr>
<tr><td colspan="6">Fer un seguiment de l'assignació de recursos i responsabilitats en gestió de seguretat de la informació per part de la direcció</td></tr>
<tr><td colspan="6">Tipus d'indicador</td></tr>
<tr><td colspan="6">Indicador de gestió</td></tr>
<tr><td colspan="2">Descripció de variables</td><td colspan="2">Formula</td><td colspan="2">Font d'informació</td></tr>
<tr><td colspan="2">X: Num. Persones amb un rol concret definit</td><td colspan="2" rowspan="2">(X/Y)*100</td><td colspan="2" rowspan="2">Arxiu de personal de recursos humans.

Actes de classificació, definició i assignació de rols i responsabilitats</td></tr>
<tr><td colspan="2">Y: Num. Persones que mantenen un rol definit al cap d'un any</td></tr>
<tr><td colspan="6">Satisfacció objectius</td></tr>
<tr><td>Mínim</td><td>75 a 80%</td><td>Satisfactori</td><td>80 a 90%</td><td>Correcte</td><td>100,00%</td></tr>
</table>

Indicador: Cobriment dels actius crítics de l'empresa relacionats amb la informació					
Identificador	SGSI_ID_2				
Definició					
Permet determinar i quantificar els actius crítics de l'empresa (relacionats directament amb la informació) ja siguin lògics o físics de l'empresa					
Objectiu					
Fer un seguiment dels actius actuals i els que s'incloguin que puguin ser crítics, analitzant així el seu nivell de protecció, privacitat i control					
Tipus d'indicador					
Indicador de gestió					
Descripció de variables		**Formula**		**Font d'informació**	
X: Num. Actius crítics exposats a un risc inacceptable		(X/Y)*100		Inventari d'actius	
Y: Num. Actius crítics totals de l'empresa					
Satisfacció objectius					
Mínim	75 a 80%	**Satisfactori**	80 a 90%	**Correcte**	100,00%

Indicador: Compliment de les polítiques de seguretat de la informació de la empresa	
Identificador	SGSI_ID_3
Definició	
Compliment de les polítiques de seguretat de la empresa	
Objectiu	
Persegueix identificar el nivell d'estructuració de cara a processos de la empresa orientats a garantir la seguretat de la informació	
Tipus d'indicador	
Indicador de compliment	
Descripció de variables	**Formula**
X: S'ha definit una política de seguretat de la informació?	X = 0 o 1
Y: S'ha definit una organització interna en termes de persones i responsabilitats amb la finalitat de complir les polítiques de seguretat de la informació i esta documentat ?	Y = 0 o 1
Z: L'empresa compleix amb els requisits legals, reglaments i contractes sobre el tractament de la informació?	Z = 0 o 1 ((X+Y+Z)/3)*100
Satisfacció objectius	

Compleix	100,00%	**No compleix**	<100%
Observacions: En cas de no complir-se alguna de les variables es considerarà que l'empresa no compleix l'objectiu de seguretat			

Indicador: Verificació controls d'accés					
Identificador		SGSI_ID_4			
Definició					
Grau de control d'accés a la informació					
Objectiu					
Persegueix identificar el grau de vulnerabilitat de la informació a accessos no autoritzats					
Tipus d'indicador					
Identificador de quantificació					
Descripció de variables		**Formula**		**Font d'informació**	
X: Num. Accessos trimestrals		(Y/X)*100		Registres d'activitat d'accessos de xarxa, servidors i equips	
Y: Num. D'alertes d'accessos no autoritzats					
Satisfacció objectius					
Mínim	40 a 100%	**Satisfactori**	10 a 40 %	**Correcte**	0,00%

Indicador: Verificació de control d'accés	
Identificador	SGSI_ID_5
Definició	
Grau de planificació de l'empresa sobre els accessos als recursos	
Objectiu	
Determinar el grau de compliment de les polítiques de seguretat de l'empresa en termes d'accés a la informació	
Descripció de variables	**Formula**
X: Hi han establerts controls d'accés lògic i físic a l'empresa?	X = 1 o 0
Y: S'han definit protocols per a definir i gestionar les credencials d'accés?	Y = 1 o 0

Satisfacció objectius					
Mínim	0 / 0 , 1 / 0	**Satisfactori**	0 / 1	**Correcte**	1 | 1

Indicador: Implementació de processos de registres i auditoria			
Identificador		SGSI_ID_6	
Definició			
Grau d'existència de processos, normes o estàndards per al registre i auditoria de la seguretat de la informació			
Objectiu			
Identificar i buscar la existència de protocols, normes o estàndards i registres d'auditoria i control de la seguretat de la informació			
Descripció de variables	**Formula**		**Font d'informació**
X: l'empresa ha definit processos d'auditoria i revisió interna i externa periodificada per als seus processos de seguretat de la informació i sistemes per assegurar el compliment de la normativa i el model de SGSI?	X = 0 o 1 Y = 0 o 1		usuaris interns de l'empresa
Y: L'empresa ha definit normes, estàndards i plans d'actuació per a garantir la seguretat de la informació, sistemes xarxes i serveis?			Direcció
Satisfacció objectius			
Compleix	1	**No compleix**	0

Indicador: Protocols de copies de seguretat		
Identificador	SGSI_ID_7	
Definició		
Avaluar si l'empresa realitza correctament copies de seguretat		
Objectiu		
Verificar el correcte plantejament de les polítiques de copies de seguretat		
Descripció de variables	**Formula**	**Font d'informació**
X: l'empresa realitza copies de seguretat periodificades?	X= 0 o 1 Y= 0 o 1	Departament informàtic

Y: l'empresa manté sistemes de seguretat per a preservar les copies de seguretat?					
Satisfacció objectius					
Mínim	0 |0 o 0| 1	**Satisfactori**	1 | 0	**Correcte**	1 | 1

Indicador: Intrusions al sistema					
Identificador			SGSI_ID_8		
Definició					
Mesura de l'eficàcia dels sistemes de control d'accés					
Objectiu					
Determinar el grau de protecció dels sistemes físics i lògics					
Descripció de variables		**Formula**			
X: num intrusions físiques		(((X/Y)*100)+((Z/K)*100))/2			
Y: num accessos permesos + accessos de serveis i autoritats					
Z: num intrusions al sistema					
K: num accessos al sistema permesos					
Satisfacció objectius					
Mínim	5 a 100%	**Satisfactori**	1 a 5%	**Correcte**	0,00%

Indicador: Grau de pèrdua d'informació					
Identificador			SGSI_ID_9		
Definició					
Quantificació i definició de les vulneracions dels documents que contenen informació de l'empresa					
Objectiu					
Control del correcte transit, cessió i gestió de la informació					
Descripció de variables		**Formula**			
X: num. Informació fugada		((X+Y+Z+K)/Num total de fitxers enviats fora de la companyia)*100			
Y: num. informació destruïda					
Z: num. informació reproduïda					
K: num informació manipulada					
Satisfacció objectius					

Mínim	5 a 100%	**Satisfactori**	1 a 5%	**Correcte**	0,00%
Indicador: Grau de pèrdua d'actius					
Identificador			SGSI_ID_10		
Definició					
Quantificació dels actius de venta (pels quals l'empresa rep remuneració)					
Objectiu					
Control del grau de pèrdues generades per la pèrdua d'actius de venta					
Descripció de variables		**Formula**			
X: num. Actius perduts per incidències en el transport		((X+Y+Z+K)/Num total d'actius de la companyia)*100			
Y: num. Actius perduts per terceres persones alienes o de la pròpia empresa					
Z: num. Actius perduts per conseqüències climatològiques					
K: num actius defectuosos					
Satisfacció objectius					
Mínim	20 a 100%	**Satisfactori**	0 a 20%	**Correcte**	0,00%

5.5 Procediment de revisió per Direcció

El sistema de Gestió de Seguretat de la Informació ha d'estar compost per un equip que s'encarregui de crear, mantenir, supervisar i millorar el Sistema. Aquest equip de treball, conegut habitualment com a Comitè de Seguretat.

Per a la correcta implantació del SGSI es necessari la definició d'aquest comitè de seguretat que, tal i com hem esmentat a les polítiques de seguretat, consta de representants de cada secció de l'empresa. En el nostre cas esta format pels següents:

- Responsable de direcció: delegat general i secretari
- Responsable de seguretat de l'organització
- Responsable de sistemes
- Responsable de Desenvolupament i projectes
- Responsable Jurídic

- Responsable de RRHH
- Responsable d'administració
- Equip d'assessors especialitzats
- Responsable comercials
- Responsable logístic

5.6 Gestió dels rols i responsabilitats

La direcció de la organització te el deure de revisar el Sistema de Gestió de Seguretat de la Informació segons la norma ISO 27001 dins d'uns intervals de temps planificats, que tenen que dur-se a terme, al menys, una vegada a l'any , assegurant que el SGSI esta correctament assegurat i es suficientment eficaç.

El principal motiu pel que sorgeix la necessitat de realitzar una revisió per part de la direcció es la de generar la garantia de que l'SGSI compleix de forma adequada, eficaç i convenient la seva missió. Aquesta revisió te que incloure l'avaluació de les oportunitats de millora i la necessitat de realitzar canvis en el SGSI, es necessari revisar la política de seguretat de la informació de la empresa i els diferents mecanismes de gestió de la seguretat de la informació.

Els resultats obtinguts de les revisions s'han de documentar, enregistrar i custodiar per a futures consultes.

Aquesta revisió es composa de punts d'entrada i punts de sortida. Els punts d'entrada definits per la norma són els següents:

1. Resultats d'auditories i revisions anteriors del SGSI
2. Observacions de les parts interessades (membres de departament)
3. Tècniques, recursos o procediments que es puguin afegir, implementar o modificar
4. Informació de les activitats preventives i correctives

5. Vulnerabilitats o amenaces
6. Resultats de mesures d'eficàcia
7. Estat de les accions iniciades en revisions anteriors
8. Qualsevol canvi que pugui afectar al SGSI
9. Recomanacions de millora

Per altra banda, el s punts de sortida son els següents:

1. Millora de l'eficàcia del SGSI
2. Actualització de la avaluació de riscos i del pla de tractament de riscos
3. Necessitats i planificació de recursos
4. Millora de mètodes de mesura de l'efectivitat dels controls
5. Modificació de procediments i controls que afecten a la seguretat de la informació.

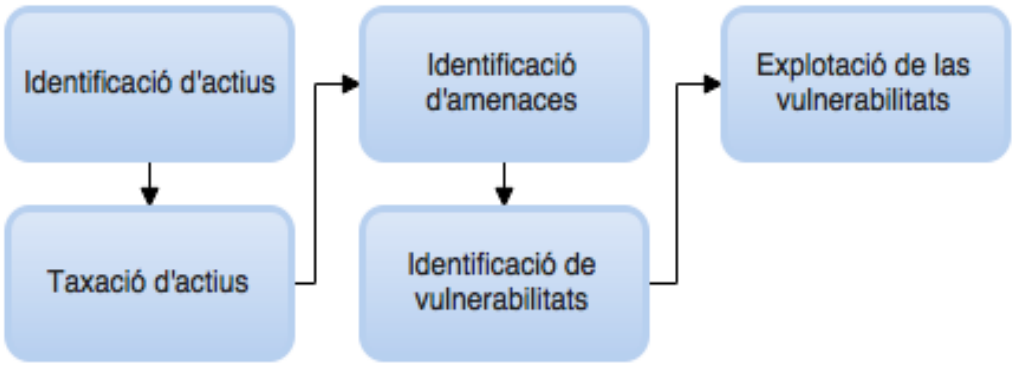
5.7 Metodologia d'anàlisi de riscos

Per a analitzar els riscos, vulnerabilitats i amenaces a les que s'exposen els actius de l'organització caldrà establir, recollir i identificar per a cada actiu les amenaces de segons les dimensions de Disponibilitat, Integritat i Confidencialitat, relacionant així el nivell de criticitat d'aquests actius en funció de si es Alta, Baixa o Mitjana, en cada cas es calcularà el total resultant de les tres dimensions (fent un valor mitja aproximat), d'aquesta manera es podrà determinar les vulnerabilitats (en funció del tipus d'actiu) relacionant la probabilitat (alta, baixa o mitjana) d'ocurrència de les amenaces pre-definides en la norma ISO en funció de si es tracta d'un actiu documental, personal, etc.

Això ens permetrà poder establir la declaració d'aplicabilitat i tenir un coneixement previ dels riscos als que s'exposen els actius valuosos de l'empresa.

En la següent taula es pot trobar la identificació i valoració dels actius així com el recull de les amenaces i vulnerabilitats dels actius; necessari per a definir i calcular el risc.

Aquest procés be il·lustrat pel següent esquema:



Taula d'Actius, amenaces i vulnerabilitats

ID	Actius	Valoració				Amenaces	Probabilitat d'ocurrència	Vulnerabilitat
		Confidencialitat	Integritat	Disponibilitat	Total			
A1	Dades de clients	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A2	Dades de proveïdors	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A3	Factures	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,B,B	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A4	Tarifes i ofertes	M	A	A	A	Falsificació, destrucció, divulgació	B,B,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A5	Inventari	M	A	A	A	Destrucció, danys parcials, robatori, pèrdua	M,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A6	Dades econòmiques de les tendes	A	A	A	A	Falsificació, destrucció, divulgació	B,B,B	Mala organització, accés no autoritzat
A7	Informació personal empleats	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,B	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A8	Software Web	A	A	A	A	Errors de codi, codi maliciós, fallades, errors usuari, fallada de seguretat	M,A,M,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A9	Software App	A	A	A	A	Errors de codi, codi maliciós, fallades, errors usuari, fallada de seguretat	M,A,M,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A10	Software terminals	A	A	A	A	Errors de codi, codi maliciós, fallades, errors usuari, fallada de seguretat	M,A,M,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A11	Hardware SSCC	A	A	A	A	Destrucció, deteriorament, danys, robatori, fallades tècniques	M,A,A,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A12	Hardware Tendes	A	A	A	A	Destrucció, deteriorament, danys, robatori, fallades tècniques	M,A,A,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A13	Hardware Centre logístic	A	A	A	A	Destrucció, deteriorament, danys, robatori, fallades tècniques	M,A,A,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat

A14	Servidors sscc i c.logistic	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A15	Base de dades clients	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A16	Base de dades productes	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A17	Base de dades proveïdors	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A18	Servidors botigues	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A19	Software de facturació	A	A	A	A	Errors de codi, codi maliciós, fallades, errors usuari, fallada de seguretat	M,A,M,B,A	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A20	Xarxa de comunicació interna	A	A	A	A	Fallades funcionament, falta de seguretat, intrusions	A,A,B	Talls de suministre, inconsistència, saturació de linies
A21	Serveis blindats de transport d'efectiu	A	A	A	A	Destrucció, danys, averies, robatori	B,M,A,M	Mal estat mecànic, falta de carburant, mala organització, falta de seguretat, personal poc qualificat
A22	Flota de distribució	M	A	A	A	Destrucció, danys, averies, robatori	B,M,A,M	Mal estat mecànic, falta de carburant, mala organització, falta de seguretat, personal poc qualificat
A23	Flota d'entrega	B	A	A	M	Destrucció, danys, averies, robatori	B,M,A,M	Mal estat mecànic, falta de carburant, mala organització, falta de seguretat, personal poc qualificat
A24	Flota comercials	B	A	A	M	Destrucció, danys, averies, robatori	B,M,A,M	Mal estat mecànic, falta de carburant, mala organització, falta de seguretat, personal poc qualificat
A25	Dades alumnes escoles	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat	B,B,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A26	Material de venta	M	A	A	A	Destrucció, danys parcials, robatori, pèrdua	M,M,A,B	Mala organització, errors en eviaments, control d'actius, clients, empleats, mala gestió dels articles
A27	Material empleats	B	A	A	M	Destrucció, danys parcials, robatori, pèrdua	M,M,M,M	Mala organització, errors en eviaments, control d'actius, clients, empleats, mala gestió dels articles
A28	Maquinària automatitzada de magatzem	M	A	A	A	Destrucció, danys, averies, robatori	M,M,A,B	Mal estat mecànic, talls elèctrics, personal poc qualificat
A29	Servidors de correu	A	A	A	A	Destrucció, danys parcials, accessos no autoritzats, alteració, intrusions, copia, divulgació	B,M,M,M,A,B,B	Personal poc qualificat, controls d'accés, fallades electriques, falta de polítiques, baixa seguretat, accés no autoritzat
A30	Instalacions SSCC	A	A	A	A	Destrucció, danys, averies, robatori, intrusions, ambientals	B,A,A,B,M,A	Fallades estructurals, mal estat estructural, mal ús, desastres climàtics, controls d'accés
A31	Instalacions centre logístic	A	A	A	A	Destrucció, danys, averies, robatori, intrusions, ambientals	B,A,A,B,M,A	Fallades estructurals, mal estat estructural, mal ús, desastres climàtics, controls d'accés
A32	Tendes	A	A	A	A	Destrucció, danys, averies, robatori, intrusions, ambientals	B,A,A,B,M,A	Fallades estructurals, mal estat estructural, mal ús, desastres climàtics, controls d'accés
A33	Dades econòmiques i contables	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A34	Treballadors	A	A	A	A	Malalties, mort, lesions	M,B,M	Mala gestió de la seguretat laboral, poca conscienciació seguretat laboral empleats, males condicions instalacions, epidemies i malalties
A35	Informació de xarxes socials	B	A	A	M	Plagi, Falsificacio, Alteracio, Destrucció	M,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control de documents
A36	Perfil de xarxes socials	B	A	A	M	Plagi, Falsificacio, Alteracio, Destrucció	M,B,A,M	Mala organització, errors en eviaments, accés no autoritzat, control d'accessos i credencials
A37	Material/mobiliari d'oficina/tenda	M	A	A	A	Destrucció, danys, averies, robatori, ambientals	B,B,B,A,M	Mal ús, deteriorament

A38	Arxiu documental fisic	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A39	Arxiu docmental lògic	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A40	Contractes de treballadors	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A41	Documentació de normativa i estructuració interna	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A42	Documentació productes pròpis	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A43	Documentació confidencial de dades de negoci	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents

Llegenda nomenclatura
A = Alta M = Mitjana B = Baixa

5.8 Declaració d'aplicabilitat

A continuació s'exposa la declaració d'aplicabilitat del procés del SGSI segons la norma ISO/IEC 27002:2013, en la que es relacionen els controls sobre els actius determinats en l'apartat anterior amb els objectius de control establerts per la norma i exposats a l'apartat Anàlisi diferencial. En aquesta taula es pretén recollir per a cadascun els controls ISO i els requeriments d'aquests si en el cas d'estudi de l'empresa XXXX s'aplica i, en cas de no aplicar-se-hi, indicar-ho.

Control ISO + requeriment	Control	comentaris	Grau d'aplicabilitat
5.1 Política de seguretat de la informació.	2		APLICA
5.1.1 Document de política de seguretat de la informació.		Redacció del document de política de seguretat	APLICA
5.1.2 Revisió de la política de seguretat de la informació.		Pla de seguretat	APLICA
6.1 Organització interna.	7		APLICA
6.1.1 Compromís de la Direcció amb la seguretat de la informació.		Conscienciació i informació als empleats membres	APLICA
6.1.2 Coordinació de la seguretat de la informació.		Formacions i Reunions directives per a anàlisi situació de la seguretat	APLICA
6.1.3 Assignació de responsabilitats relatives a la seg. de la informació.		Documentació, assignació de responsabilitats i comitè	APLICA
6.1.4 Procés d'autorització de recursos per al tractament de la informació.		Establerta jerarquia i correctament documentada	APLICA
6.1.5 Acords de confidencialitat.		documentació	APLICA
6.1.6 Contacte amb les autoritats.		Protocols d'actuació davant d'incompliments legals	APLICA

6.1.7 Contacte amb grups d'especial interès.			APLICA
6.1.8 Revisió independent de la seguretat de la informació.		Avaluar: Protocols, salvaguardes i mecanismes de seguretat	APLICA
6.2 Tercers.	3		APLICA
6.2.1 Identificació dels riscos derivats de l'accés de tercers.		Protocols i filtres per enviament de documentació a terceres parts	APLICA
6.2.2 Tractament de la seguretat en la relació amb els clients.		Formació empleats i protocols per al lliurament d'informació a clients	APLICA
6.2.3 Tractament de la seguretat en contractes amb tercers.		Protocols i filtres per enviament de documentació a terceres parts	APLICA
7.1 Responsabilitat sobre els actius.	2		APLICA
7.1.1 Inventari d'actius.		Documentació i glossari d'actius de l'empresa	APLICA
7.1.2 Propietat dels actius.			APLICA
7.1.3 Ús acceptable dels actius.		Normativa aplicada a l'ús i formació dels responsables del seu ús	APLICA
7.2 Classificació de la informació.	2		APLICA
7.2.1 Directrius de classificació.		Redacció documentació relativa a la classificació de la informació	APLICA
7.2.2 Etiquetatge i manipulat de la informació.		Mecanismes d'etiquetatge i protocols implantats per a això	APLICA
8.1 Abans de l'ocupació.	2		APLICA

8.1.1 Funcions i responsabilitats.			APLICA
8.1.2 Investigació d'antecedents.		Supervisió protocols d'investigació seguint la legislació vigent	APLICA
8.1.3 Condicions de contractació.		Redacció contractes i precontractes	APLICA
8.2 Durant l'ocupació.	1		APLICA
8.2.1 Responsabilitats de la Direcció.			APLICA
8.2.2 Conscienciació, formació i capacitació en seg. de la informac.		Protocols i sistemes de formació i conscienciació	APLICA
8.2.3 Procés disciplinari.		Redacció document de sancions i infraccions	APLICA
8.3 Cessament de l'ocupació o canvi de lloc de treball.	2		APLICA
8.3.1 Responsabilitat del cessament o canvi.			APLICA
8.3.2 Devolució d'actius.		Protocol de devolució d'actius	SOLAMENT PALICA ALS COMERCIALS I ALTRES TREBALLADORS QUE TINGUIN UN VEHICLE A CÀRREC
8.3.3 Retirada dels drets d'accés.		Protocol i demora dels processos de retirada d'accessos	APLICA
9.1 Àrees segures.	5		APLICA
9.1.1 Perímetre de seguretat física.		Existència i eficiència sistemes perimetrals	APLICA
9.1.2 Controls físics d'entrada.		Existència i eficiència accessos	APLICA
9.1.3 Seguretat d'oficines, despatxos i instal·lacions.		Existència i eficiència accessos	APLICA

9.1.4 Protecció contra les amenaces externes i d'origen ambiental.		Existència de sensors d'humitat, fum i / o elèctrics	APLICA
9.1.5 Treball en àrees segures.			APLICA
9.1.6 Àrees d'accés públic i de càrrega i descàrrega.		Correcta gestió d'accés i vigilància	APLICA
9.2 Seguretat dels equips.	3		APLICA
9.2.1 Emplaçament i protecció d'equips		Mesures de seguretat físiques i lògiques	APLICA
9.2.2 Instal·lacions de subministrament.			APLICA
9.2.3 Seguretat del cablejat.			APLICA
9.2.4 Manteniment dels equips.		Planificació tasques manteniment	APLICA
9.2.5 Seguretat dels equips fora de les instal·lacions.		Mesures d'identificació d'equips mòbils	APLICA
9.2.6 Re-utilització o retirada segura d'equips.			APLICA
9.2.7 Retirada de materials propietat de l'empresa.			APLICA (DOCUMENTACIÓ A DESTRUCCIÓ SEGURA)
10.1 Responsabilitats i procediments d'operació.	0		APLICA
10.1.1 Documentació dels procediments d'operació.			APLICA
10.1.2 Gestió de canvis.			APLICA
10.1.3 Segregació de tasques.			APLICA
10.1.4 Separació dels recursos de desenvolupament, prova i operació.			APLICA
10.2 Gestió de la provisió de serveis per tercers.	0		APLICA
10.2.1 Provisió de serveis.			APLICA
10.2.2 Supervisió i revisió dels serveis prestats per tercers.			APLICA
10.2.3 Gestió del canvi en els serveis prestats per			APLICA

tercers.			
10.3 Planificació i acceptació del sistema.	0		APLICA
10.3.1 Gestió de capacitats.			APLICA
10.3.2 Acceptació del sistema.			APLICA
10.4 Protecció contra el codi maliciós i descarregable.	1		APLICA
10.4.1 Controls contra el codi maliciós.		Implantació i manteniment de sistemes Programari per a la detecció d'intrusions i desenvolupament d'actualitzacions de seguretat per a programari propi	APLICA
10.4.2 Controls contra el codi descarregat al client.			NO S'APLICA, ELS CLIENTS NO PODEN DESCARREGAR CAP TIPUS DE CODI NI FITXER, JA QUE ES REMETEN A CONSULTAR I COMPRAR PER INTERNET I ALTRES PLATAFORMES VIRTUALS (MAI ES INSTAL LEN SOFTWARE DE L'EMPRESA EN ELS SEUS TERMINALS PROPIS)
10.5 Còpies de seguretat.	1		APLICA
10.5.1 Còpies de seguretat de la informació.		Protocol i periodicitat de còpies de seguretat. Correcte emmagatzematge de les còpies de seguretat.	APLICA
10.6 Gestió de la seguretat de les xarxes.	2		APLICA
10.6.1 Controls de xarxa.		Tallafocs i accessos amb acreditació d'empleat	APLICA

10.6.2 Seguretat dels serveis de xarxa.		Seguretat en serveis web amb e-comerç	APLICA
10.7 Manipulació dels suports.	1		APLICA
10.7.1 Gestió de suports extraïbles.			APLICA
10.7.2 Retirada de suports.			APLICA
10.7.3 Procediments de manipulació de la informació.			APLICA
10.7.4 Seguretat de la documentació del sistema.		Gestió i assignació de rols i credencials	APLICA
10.8 Intercanvi d'informació.	2		APLICA
10.8.1 Polítiques i procediments d'intercanvi d'informació.		Redacció de protocols, normes i polítiques d'intercanvi	APLICA (DE CARA A CLIENTS I TERCERS)
10.8.2 Acords d'intercanvi.			NO APLICA, L'EMPRESA NO CEDEIX MES QUE LES DADES QUE PRÈVIAMENT HAN ESTAT CEDITS PER ALS CLIENTS per a PODER SER TRASLLADAT A PROVEÏDORS
10.8.3 Suports físics en trànsit.			NO APLICA, L'MEPRESA NO TRASLLADA INFORMACIÓ PER MITJÀ AQUEST TIPUS DE SUPORTS
10.8.4 Missatgeria electrònica.		Redacció i control d'ús de servidors de correu electrònic	APLICA
10.8.5 Sistemes d'informació empresarials.			APLICA
10.9 Serveis de comerç electrònic.	3		APLICA
10.9.1 Comerç electrònic.		Redacció i informació als clients segons normativa vigent	APLICA
10.9.2 Transaccions en línia.		Seguretat, contractes i tractament de la	APLICA

		informació	
10.9.3 Informació públicament disponible.		Supervisió informació pública sobre transaccions	APLICA
10.10 Supervisió.	1		APLICA
10.10.1 Registres d'auditoria.		Planing d'auditories internes	APLICA
10.10.2 Supervisió de l'ús del sistema.			APLICA
10.10.3 Protecció de la informació dels registres.			APLICA
10.10.4 Registres d'administració i operació.			APLICA
10.10.5 Registre de fallades.			APLICA
10.10.6 Sincronització del rellotge.			NO APLICA, EN AQUEST CAS D'ESTUDI L'MEPRESA NO GESTIONA AQUEST ASPECTE COM UNA RESPONSABILITAT O OBJECTIU DE NEGOCI
11.1 Requisits de negoci per al control d'accés.	1		APLICA
11.1.1 Política de control d'accés.		Redacció de la política de control d'accessos	APLICA
11.2 Gestió d'accés d'usuari.	2		APLICA
11.2.1 Registre d'usuari.			APLICA
11.2.2 Gestió de privilegis.		Normes i documentació dels privilegis, amb polítiques d'assignació segons responsabilitats i càrrec en l'empresa	APLICA
11.2.3 Gestió de contrasenyes d'usuari.		Premisses de seguretat per a establiment de contrasenyes	APLICA

11.2.4 Revisió dels drets d'accés d'usuari.			APLICA
11.3 Responsabilitats d'usuari.	2		APLICA
11.3.1 Ús de contrasenyes.			APLICA
11.3.2 Equip d'usuari desatès.		Mesures de no intrusió a equips encesos amb sessions iniciades	APLICA
11.3.3 Política de lloc de treball buidat i pantalla neta.		Redacció de normes de neteja	APLICA
11.4 Control d'accés a la xarxa.	1		APLICA
11.4.1 Política d'ús dels serveis en xarxa.		Redacció de normes d'ús i accés de serveis de xarxa	APLICA
11.4.2 Autenticació d'usuari per a connexions externes.			APLICA
11.4.3 Identificació dels equips en les xarxes.			APLICA
11.4.4 Protecció dels ports de diagnòstic i configuració remots.			APLICA
11.4.5 Segregació de les xarxes.			APLICA
11.4.6 Control de la connexió a la xarxa.			APLICA
11.4.7 Control d'encaminament (routing) de xarxa.			APLICA
11.5 Control d'accés al sistema operatiu.	3		APLICA
11.5.1 Procediments segurs d'inici de sessió.			APLICA
11.5.2 Identificació i autenticació d'usuari.		Desenvolupament de sistema d'inici de sessió d'usuari	APLICA
11.5.3 Sistema de gestió de contrasenyes.		Caducitat i re-establiment de contrasenyes	APLICA
11.5.4 Ús dels recursos del sistema.			APLICA

11.5.5 Desconnexió automàtica de sessió.		Timers de des-connexió automàtica	APLICA
11.5.6 Limitació del temps de connexió.			APLICA
11.6 Control d'accés a les aplicacions i a la informació.	1		APLICA
11.6.1 Restricció de l'accés a la informació.		Accessos amb sistemes de restricció segons credencials i responsabilitats assignades	APLICA
11.6.2 Aïllament de sistemes sensibles.			APLICA
11.7 Ordinadors portàtils i teletreball.	1		APLICA
11.7.1 Ordinadors portàtils i comunicacions mòbils.		Identificació d'usuaris i assignació d'usuari únic com a propietari de l'equip	APLICA
11.7.2 Teletreball.			NO APLICA, EN AQUESTA EMRPESA NO ES PERMET EL TELETREBALL CONSIDERANT QUE ELS COMERCIALS QUE DESPLACEN NO ABANDONEN EL SEU LLOC DE TREBALL, ÉS A DIR, NO ES DIRIGEIXEN NI S'UBIQUEN A TREBALLAR ON ELLS ESCULLIN, SI NO QUE EXERCEIXEN SEGONS ELS CLIENTS I URGÈNCIES COMERCIALS QUE SORGIN
12.1 Requisits de seguretat dels sistemes d'informació.	1		APLICA
12.1.1 Anàlisi i especificació dels requisits de seguretat.		Validació requisits correctament documentats i implantats	APLICA
12.2 Tractament correcte de les aplicacions.	0		APLICA
12.2.1 Validació de les			APLICA

dades d'entrada.			
12.2.2 Control del processament intern.			APLICA
12.2.3 Integritat dels missatges.			APLICA
12.2.4 Validació de les dades de sortida.			APLICA
12.3 Controls criptogràfics.	0		
12.3.1 Política d'ús dels controls criptogràfics.			APLICA
12.3.2 Gestió de claus.			APLICA
12.4 Seguretat dels arxius de sistema.	3		APLICA
12.4.1 Control del programari en explotació.		Implantació sistema de credencials i autoritzacions	NO APLICA, NO DISPOSEN DE SOFTWARE D'EXPLOTACIÓ, NOMÉS SOFTWARE D'ÚS PROPI O AMB COMPRA D'LLICÈNCIA A ALTRES EMPRESES
12.4.2 Protecció de les dades de prova del sistema.		Implantació sistema de credencials i autoritzacions	APLICA
12.4.3 Control d'accés al codi font dels programes.		Implantació sistema de credencials i autoritzacions	APLICA
12.5 Seguretat en els processos de desenvolupament i suport.			APLICA
12.5.1 Procediments de control de canvis.		Implantació sistema de credencials i autoritzacions. Registre de modificacions	APLICA
12.5.2 Revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu.			
12.5.3 Restriccions als canvis en els paquets de programari.			
12.5.4 Fuites d'informació.			
12.5.5 Externalització del desenvolupament de programari.			

12.6 Gestió de la vulnerabilitat tècnica.	0		APLICA
12.6.1 Control de les vulnerabilitats tècniques.			APLICA
13.1 Notificació d'esdeveniments i punts febles de seguretat de la informació.	2		APLICA
13.1.1 Notificació dels esdeveniments de seguretat de la informació.		Sistemes d'alertes de seguretat	APLICA
13.1.2 Notificació de punts febles de seguretat.		Documentació i avaluació iterativa	APLICA
13.2 Gestió d'incidents i millores de seguretat de la informació.	2		APLICA
13.2.1 Responsabilitats i procediments.		Assignació de responsabilitats i documentació	APLICA
13.2.2 Aprenentatge dels incidents de seguretat de la informació.			APLICA
13.2.3 Recull d'evidències.		Documentació i avaluació iterativa	APLICA
14.1 Aspectes de seguretat de la informació en la gestió de la continuïtat del negoci.	5		APLICA
14.1.1 Inclusió de la seguretat de la informació en el procés de gestió de la continuïtat del negoci.		Control reunions directives i documentació	APLICA
14.1.2 Continuïtat del negoci i avaluació de riscos.		Control reunions directives i documentació	APLICA
14.1.3 Desenvolupament i implantació de plans de continuïtat que incloguin la seguretat de la informació.		Control reunions directives i documentació	APLICA
14.1.4 Marc de referència per a la planificació de la continuïtat del negoci.		Control reunions directives i documentació	APLICA
14.1.5 Proves, manteniment i re-avaluació de plans de		Control reunions directives i documentació	APLICA

continuïtat.			
15.1 Compliment dels requisits legals.	6		APLICA
15.1.1 Identificació de la legislació aplicable.		Control reunions directives i documentació	APLICA
15.1.2 Drets de propietat intel·lectual (DPI).		Control reunions directives i documentació	APLICA
15.1.3 Protecció dels documents de l'organització.		Control reunions directives i documentació	APLICA
15.1.4 Protecció de dades i privacitat de la informació de caràcter personal.		Control reunions directives i documentació	APLICA
15.1.5 Prevenció de l'ús indegut de recursos de tractament de la informació.		Control reunions directives i documentació	APLICA
15.1.6 Regulació dels controls criptogràfics.		Control reunions directives i documentació	APLICA
15.2 Compliment de les polítiques i normes de seguretat i compliment tècnic.	1		APLICA
15.2.1 Compliment de les polítiques i normes de seguretat.		Revisió i redacció de les normes i polítiques de seguretat	APLICA
15.2.2 Prova de conformitat tècnic.		comentaris	APLICA
15.3 Consideracions sobre les auditories dels sistem. d'informació.	0		APLICA
15.3.1 Controls d'auditoria dels sistemes d'informació.		Redacció del document de política de seguretat	APLICA
15.3.2 Protecció de les eines d'auditoria dels sist. d'inform.		Pla de seguretat	APLICA

6. Anàlisi de riscos

6.1 Introducció

Per tal de poder protegir els actius de l'empresa, que a priori no coneixem, cal com a primera etapa del pla d'implementació d'un Sistema Gestor de la Seguretat de la Informació (SGSI) avaluar els actius de l'empresa i considerar les dependències entre ells i fent una valoració d'aquests per a poder arribar a establir l'estat de la seguretat dels actius. Per a fer-ho s'han de determinar i realitzar un seguit de càlculs per tal d'obtenir els actius que s'haurà d'avaluar i classificar, els riscos als que estan sotmesos, el nivell de vulnerabilitat i a quin tipus de dimensió respon aquesta vulnerabilitat, per així poder iniciar un projecte de millora del nostre sistema gestor.

A continuació, en aquest apartat es poden observar els diferents passos a seguir i els resultats obtinguts per l'empresa XXXX i el seu SGSI.

6.2 Inventari d'actius

A continuació es recullen els actius necessaris per a poder iniciar l'estudi d'aquests i així iniciar l'anàlisi de riscos. Aquests actius es veuen agrupats segons Magerit en categories (Instal·lacions, Hardware, Aplicació, Dades, Xarxa, Serveis, Equipament auxiliar i Personal):

Àmbit	Actiu
Dades	Dades de clients
Dades	Dades de proveïdors
Dades	Factures
Dades	Tarifes i ofertes
Dades	Inventari
Dades	Dades econòmiques de les tendes
Dades	Informació personal empleats
Aplicació	Software Web
Aplicació	Software App
Aplicació	Software terminals
Hardware	Hardware SSCC
Hardware	Hardware Tendes
Hardware	Hardware Centre logístic
Serveis	Servidors sscc i c.logistic
Dades	Base de dades clients
Dades	Base de dades productes
Dades	Base de dades proveïdors
Xarxa	Servidors botigues
Aplicació	Software de facturació
Xarxa	Xarxa de comunicació interna
Equipament auxiliar	Serveis blindats de transport d'efectiu
Equipament auxiliar	Flota de distribució
Equipament auxiliar	Flota d'entrega
Equipament auxiliar	Flota comercials
Dades	Dades alumnes escoles
Aplicació	Material de venta
Aplicació	Material empleats
Hardware	Maquinària automatitzada de magatzem
Xarxa	Servidors de correu
Instal·lacions	Instalacions SSCC
Instal·lacions	Instalacions centre logístic
Instal·lacions	Tendes
Dades	Dades econòmiques i contables
Personal	Treballadors
Xarxa	Informació de xarxes socials
Aplicació	Perfil de xarxes socials
Instal·lacions	Material/mobiliari d'oficina/tenda
Instal·lacions	Arxiu documental fisic
Dades	Arxiu docmental lògic
Personal	Contractes de treballadors
Aplicació	Documentació de normativa i estructuració interna
Dades	Documentació productes pròpis
Dades	Documentació confidencial de dades de negoci
Serveis	Subministre electric
Serveis	Subministre d'internet i telefon
Serveis	Subministre aigua
Equipament auxiliar	Sistemes de seguretat (tendes i altres edificis)

6.3 Valoració d'actius

A continuació es procedeix a la distinció i separació dels diferents actius citats classificant-los i jerarquitzant-los en funció de l'impacte que suposaria un incident sobre aquests actius. La següent taula classifica i il·lustra aquesta classificació, seguint la classificació que proposa Magerit.

Actiu	Valoració
Dades de clients	6
Dades de proveïdors	6
Factures	3
Tarifes i ofertes	7
Inventari	3
Dades econòmiques de les tendes	6
Informació personal empleats	6
Software Web	9
Software App	9
Software terminals	9
Hardware SSCC	8
Hardware Tendes	9
Hardware Centre logístic	7
Servidors sscc i c.logistic	9
Base de dades clients	7
Base de dades productes	7
Base de dades proveïdors	5
Servidors botigues	7
Software de facturació	8
Xarxa de comunicació interna	6
Serveis blindats de transport d'efectiu	9
Flota de distribució	7
Flota d'entrega	5
Flota comercials	3
Dades alumnes escoles	6
Material de venta	2
Material empleats	1
Maquinària automatitzada de magatzem	6
Servidors de correu	5
Instalacions SSCC	8
Instalacions centre logístic	8
Tendes	8
Dades econòmiques i contables	8
Treballadors	6
Informació de xarxes socials	2
Perfil de xarxes socials	2
Material/mobiliari d'oficina/tenda	1
Arxiu documental fisic	5
Arxiu docmental lògic	5
Contractes de treballadors	7
Documentació de normativa i estructuració interna	8
Documentació productes pròpis	8
Documentació confidencial de dades de negoci	9
Subministre electric	5
Subministre d'internet i telefon	5
Subministre aigua	1
Sistemes de seguretat (tendes i altres edificis)	7
Molt alt	Mig
Alt	Baix

6.4. Dimensions de seguretat

Des de el punt de vista de la seguretat, junt a l'anterior valoració dels actius descrits, s'ha de realitzar la valoració ACIDA, és a dir, determinar i valorar la criticitat dels actius en les cinc dimensions de la seguretat de la Informació que gestiona el procés de negoci. Aquesta valoració compren el detall de les cinc dimensions de seguretat que, a diferència que en l'apartat anterior, es una valoració més profunda, en lloc d'una simple estimació.

El valor que s'assignarà a cada actiu pot ser propi o acumulat, és adir, ser el resultat del valor d'actius inferiors en una jerarquia o ser el del propi actiu (com a unitari). Així mateix, cada actiu pot tenir uns valors en cada dimensió independents en relació a altres, per tant, uns actius no depenen dels altres a l'hora de valorar les cinc dimensions A C I D A.

Un cop determinades les dimensions es necessari mencionar i establir l'escala de valoració d'aquestes dimensions, que ve exemplificada en la taula següent:

Valor	Criteri: segons el dany a l'organització
10	Dany molt greu
7-9	Dany greu
4-6	Dany important
1-3	Dany menor
0	Dany irrellevant

Partint de les valoracions i criteris establerts, es valoraran aquests actius amb importància molt alta, alta, mitjana, baixa o irrellevant a la vegada que s'assignarà a cada actiu en cada dimensió una valoració sobre 10 i es presentaran els resultats en la següent taula.

Àmbit	Actiu	Valor	Auditabilitat	Confidencialita	Integritat	Disponibilitat	Autenticitat
Dades	Dades de clients	9,8	10	10	10	9	10
Dades	Dades de proveïdors	8,4	9	10	9	7	7
Dades	Factures	4,2	5	5	6	1	4
Dades	Tarifes i ofertes	4	3	5	6	1	5
Dades	Inventari	2,2	2	2	3	2	2
Dades	Dades econòmiques de les tendes	2,8	2	3	3	1	5
Dades	Informació personal empleats	7,4	5	10	7	5	10
Aplicació	Software Web	9	9	8	10	10	8
Aplicació	Software App	8,8	9	8	10	9	8
Aplicació	Software terminals	8,4	10	8	10	9	5
Hardware	Hardware SSCC	6,8	7	4	10	8	5
Hardware	Hardware Tendes	7,2	8	5	10	9	4
Hardware	Hardware Centre logístic	6	5	4	10	7	4
Serveis	Servidors sscc i c.logistic	6,8	6	4	10	10	4
Dades	Base de dades clients	9,6	9	10	10	10	9
Dades	Base de dades productes	8,8	7	10	10	9	8
Dades	Base de dades proveïdors	8,6	7	10	10	8	8
Xarxa	Servidors botigues	7,8	9	6	10	10	4
Aplicació	Software de facturació	9,6	10	9	10	10	9
Xarxa	Xarxa de comunicació interna	7	9	2	7	8	9
E.auxiliar	Serveis blindats de transport d'efectiu	7	6	9	10	10	0
E.auxiliar	Flota de distribució	5,2	2	8	7	9	0
E.auxiliar	Flota d'entrega	3,2	1	3	6	6	0
E.auxiliar	Flota comercials	2	1	1	3	5	0
Dades	Dades alumnes escoles	7,2	5	10	8	6	7
Aplicació	Material de venta	5,2	0	7	10	6	3
Aplicació	Material empleats	0,4	0	0	0	0	2
Hardware	Maquinària automatitzada de magatzem	3,2	2	4	5	4	1
Xarxa	Servidors de correu	4,2	8	3	6	3	1
Instal·lacions	Instalacions SSCC	3,6	9	1	7	1	0
Instal·lacions	Instalacions centre logístic	3,8	9	1	7	2	0
Instal·lacions	Tendes	6,4	10	5	8	9	0
Dades	Dades econòmiques i contables	6	8	6	4	5	7
Personal	Treballadors	6,2	5	6	8	10	2
Xarxa	Informació de xarxes socials	1,8	1	0	3	0	5
Aplicació	Perfil de xarxes socials	1,2	2	1	2	0	1
Instal·lacions	Material/mobiliari d'oficina/tenda	0,4	0	0	1	1	0
Instal·lacions	Arxiu documental fisic	4,8	6	2	7	2	7
Dades	Arxiu docmental lògic	5,8	8	2	8	6	5
Personal	Contractes de treballadors	6,2	7	8	7	4	5
Aplicació	Documentació de normativa i estructuració interna	5,8	10	7	2	5	5
Dades	Documentació productes pròpis	4	7	5	2	3	3
Dades	Documentació confidencial de dades de negoci	6,4	10	8	3	3	8
Serveis	Subministre electric	2,8	2	0	2	8	2
Serveis	Subministre d'internet i telefon	2,8	2	0	2	8	2
Serveis	Subministre aigua	1,6	2	0	1	3	2
E.auxiliar	Sistemes de seguretat (tendes i altres edificis)	8	10	9	10	9	2

Molt Greu
Greu
Important
Menor
Irrellevant

6.5 Anàlisi d'amenaces

Tots els actius estan exposats a amenaces, les quals, poden afectar a diferents aspectes de la seguretat d'aquests. Es pretén analitzar quines amenaces poden afectar a quins actius, partint de l'estudi es podrà determinar la vulnerabilitat de cada actiu respecte a les amenaces potencials. Per a dur a terme aquest enfoc es disposarà una taula inicial amb 4 tipus d'amenaces, sent aquestes les amenaces descrites per MAGERIT (llibre II punt 5); aquestes amenaces són les següents.

Amenaces	Identificador Amenaces
Desastres Naturals	DN
D'origen Industrial	OI
Errors i Fallides No Intencionats	NI
Atacs Intencionats	AI

A continuació s'exposen per a cada tipologia d'amenaça indicades en la taula superior la freqüència d'ocurrència i el nivell d'afectació a les diferents dimensions de la seguretat.

Àmbit	Actiu	Freqüència	Autenticitat	Confidencialitat	Integritat	Disponibilitat	Trassabilitat
Dades	Dades de clients	20	25	45,3	33	30	7,5
	DN					1	
	OI			1		20	
	NI			80	50	40	30
	AI		100	100	80	60	
Dades	Dades de proveïdors	15	25	45,3	30	28	7,5
	DN					1	
	OI			1		20	
	NI			80	50	30	30
	AI		100	100	70	60	
Dades	Factures	40	25	45,3	33	28	15
	DN					1	
	OI			1		20	
	NI			80	50	30	30
	AI		100	100	80	60	30
Dades	Tarifes i ofertes	2	17,5	25,3	23	25	5
	DN					1	
	OI			1		10	
	NI			20	10	10	20
	AI		70	80	80	80	

	Inventari	10	15	22,8	20	25	10
	DN					1	
Dades	OI			1		10	
	NI			30	20	20	40
	AI		60	60	60	70	
	Dades econòmiques de les tendes	3	17,5	7,75	23	18	6,3
	DN					1	
Dades	OI			1		10	
	NI			10	20	30	5
	AI		70	20	70	30	20
	Informació personal empleats	1	7,5	40	7,5	7,5	0
	DN						
Dades	OI						
	NI			60			
	AI		30	100	30	30	
	Software Web	2	12,5	37,5	38	45	7,5
	DN						
Aplicació	OI					30	
	NI			50	50	50	10
	AI		50	100	100	100	20
	Software App	1	12,5	37,5	38	45	7,5
	DN						
Aplicació	OI					30	
	NI			50	50	50	10
	AI		50	100	100	100	20
	Software terminals	0	12,5	37,5	38	43	7,5
	DN						
Aplicació	OI					20	
	NI			50	50	50	10
	AI		50	100	100	100	20
	Hardware SSCC	5	0	17,5	18	80	2,5
	DN					100	
Hardware	OI					100	
	NI			30	40	60	10
	AI			40	30	60	
	Hardware Tendes	70	0	17,5	18	80	2,5
	DN					100	
Hardware	OI					100	
	NI			30	40	60	10
	AI			40	30	60	
	Hardware Centre logístic	5	0	17,5	18	80	2,5
	DN					100	
Hardware	OI					100	
	NI			30	40	60	10
	AI			40	30	60	
	Servidors sscc i c.logistic	3	2,5	25	30	25	2,5
	DN						
Serveis	OI						
	NI			40	60	60	
	AI		10	60	60	40	10
	Base de dades clients	120	25	45,3	33	30	10
	DN					1	
Dades	OI			1		20	
	NI			80	50	40	30
	AI		100	100	80	60	10

Dades	Base de dades productes	150	25	37,8	33	30	10
	DN					1	
	OI			1		20	
	NI			50	50	40	30
	AI		100	100	80	60	10
	Base de dades proveïdors	12	25	45,3	33	30	10
Aplicació	Material empleats	70	5	15	15	40	2,5
	DN					50	
	OI					50	
	NI			50	50	50	10
	AI		20	10	10	10	
Hardware	Maquinària automatitzada de magatzem	2	0	17,5	18	80	2,5
	DN					100	
	OI					100	
	NI			30	40	60	10
	AI			40	30	60	
Xarxa	Servidors de correu	7	15	42,5	40	48	20
	DN						
	OI					30	
	NI			70	60	60	10
	AI		60	100	100	100	70
Instal·lacions	Instalacions SSCC	2	0	57,5	38	100	0
	DN					100	
	OI			30		100	
	NI			100	100	100	
	AI			100	50	100	
Instal·lacions	Instalacions centre logístic	3	0	57,5	38	100	0
	DN					100	
	OI			30		100	
	NI			100	100	100	
	AI			100	50	100	
Instal·lacions	Tendes	3	0	57,5	38	100	0
	DN					100	
	OI			30		100	
	NI			100	100	100	
	AI			100	50	100	
Dades	Dades econòmiques i contables	1	25	35,3	7,5	35	5
	DN					1	
	OI			1		20	
	NI			40		40	10
	AI		100	100	30	80	10
Personal	Treballadors	70	0	0	0	33	0
	DN						
	OI						
	NI					50	
	AI					80	
Xarxa	Informació de xarxes socials	1	12,5	7,5	15	23	7,5
	DN						
	OI					30	
	NI			10	10	10	10
	AI		50	20	50	50	20
Aplicació	Perfil de xarxes socials	1	32,5	0	0	33	0
	DN						
	OI						
	NI		50			50	
	AI		80			80	
Instal·lacions	Material/mobiliari d'oficina/tenda	45	0	0	50	100	0
	DN					100	
	OI					100	
	NI				100	100	
	AI				100	100	

Instal·lacions	Arxiu documental fisic	3	0	57,5	38	100	0
	DN					100	
	OI			30		100	
	NI			100	100	100	
	AI			100	50	100	
Dades	Arxiu docmental lògic	10	25	35,3	28	35	5
	DN					1	
	OI			1		20	
	NI			40	40	40	10
	AI		100	100	70	80	10
Personal	Contractes de treballadors	0	2,5	15,3	7,5	10	5
	DN					1	
	OI			1		20	
	NI			10	10	10	10
	AI		10	50	20	10	10
Aplicació	Documentació de normativa i estructuració interna	0	0	40	0	40	0
	DN					10	
	OI					50	
	NI			80		50	
	AI			80		50	
Dades	Documentació productes pròpis	3	0	0	0	40	0
	DN					10	
	OI					50	
	NI					50	
	AI					50	
Dades	Documentació confidencial de dades de negoci	0	0	40	0	40	0
	DN					10	
	OI					50	
	NI			80		50	
	AI			80		50	
Serveis	Subministre electric	4	2,5	22,5	28	73	2,5
	DN					100	
	OI					90	
	NI			40	60	60	
	AI		10	50	50	40	10
Serveis	Subministre d'internet i telefon	15	2,5	25	30	73	2,5
	DN					100	
	OI					90	
	NI			40	60	60	
	AI		10	60	60	40	10
Serveis	Subministre aigua	3	2,5	22,5	28	73	2,5
	DN					100	
	OI					90	
	NI			40	60	60	
	AI		10	50	50	40	10
Equipament auxiliar	Sistemes de seguretat (tendes i altres edificis)	1	0	40	25	100	25
	DN					100	
	OI			50		100	
	NI			10	50	100	50
	AI			100	50	100	50

Per analitzar les amenaces s'han exposat de forma genèrica en funció de les famílies d'amenaces exposades en la primera taula d'aquest apartat, però s'han tingut en compte totes les amenaces concretes de cada família definides per magerit, que en són les següents, on les dimensions son les primeres lletres de les dimensions de la taula anterior.

Desastres naturals	
Tipologia	Dimensió a la que afecten
Foc	D
Danys per aigua	D
Altres desastres naturals	D

Origen Industrial	
Tipologia	Dimensió a la que afecten
Foc	D
Danys per aigua	D
Danys industrials	D
Degradació dels suports d'emmagatzemament d'informació	D
Contaminació mecànica	D
Contaminació electromagnètica	D
Averia física o lògica	D
Tall de subministres elèctric	D
Condicions de temperatura o humitat inadequades	D
Fallades de serveis de comunicacions	D
Interrupció d'altres serveis i subministres	D
Emanacions electromagnètiques	C

Errors i Danys no intencionats	
Tipologia	Dimensió a la que afecten
Errors usuaris	I, C, D
Errors Administrador	D, I, C
Errors monitorització	T
Errors configuració	I
Deficiències de l'organització	D
Difusió de software perjudicial	D, I, C
Errors de re-/encaminament	C
Errors de seqüència	I
Fugues d'informació	C
Alteracions accidentals d'informació	I
Destrucció d'informació	D
Vulnerabilitats dels programes	I, D, C
Errors de manteniment / actualització de programes	I, D
Errors de manteniment / actualització de hardware	D
Caigudes del sistema causades per esgotament de recursos	D
Pèrdua d'equips	D, C
In-disponibilitat del personal	D

Atacs intencionats	
Tipologia	Dimensió a la que afecten
Suplantació d'identitat d'usuari	C, A, I
Manipulació configuració	I , C, A
Manipulació logs del sistema	T
Abús de privilegis d'accés	C, I ,D
Ús no previst	D, C , I
Difusió de software maliciós	D , I ,C
Re-/encaminament missatges	C
Alteració de seqüencies	I
Accés no autoritzat	C, I
Anàlisis de tràfic	C
Repudi	T
Modificació d'informació	I
Intercepció d'informació	C
Destrucció d'informació	D
Divulgació d'informació	C
Manipulació d'equips	C, D
Manipulació de programes	C, I , D
Denegació de servei	D
Robatori	D, C
Atac destructiu	D
Ocupació enemiga	D, C
In-disponibilitat del personal	D
Extorsió	C, I , D

6.6 Impacte potencial

El següent pas a dur a terme es el càlcul de l'impacte que suposaria que les amenaces sobre els actius (en funció de la seva ocurrència) es materialitzin en funció del valor de cada actiu, poden així obtenir una valoració de la gravetat de l'impacte que suposaria per a l'organització. A continuació es poden veure les valoracions (obre 10) de l'impacte per a cada actiu descrit anteriorment.

Àmbit	Actiu	Freqüència	Autenticitat	Confidencialitat	Integritat	Disponibilitat	Trassabilitat	Valor	Valoració Impacte
Dades	Dades de clients	20	25	45,25	32,5	30,25	7,5	9,8	ALTA
Dades	Dades de proveïdors	15	25	45,25	30	27,75	7,5	8,4	ALTA
Dades	Factures	40	25	45,25	32,5	27,75	15	4,2	MITJA
Dades	Tarifes i ofertes	2	17,5	25,25	22,5	25,25	5	4	MITJA
Dades	Inventari	10	15	22,75	20	25,25	10	2,2	MITJA
Dades	Dades econòmiques de les tendes	3	17,5	7,75	22,5	17,75	6,25	2,8	BAIXA
Dades	Informació personal empleats	1	7,5	40	7,5	7,5	0	7,4	ALTA
Aplicació	Software Web	2	12,5	37,5	37,5	45	7,5	9	ALTA
Aplicació	Software App	1	12,5	37,5	37,5	45	7,5	8,8	ALTA
Aplicació	Software terminals	0	12,5	37,5	37,5	42,5	7,5	8,4	ALTA
Hardware	Hardware SSCC	5	0	17,5	17,5	80	2,5	6,8	ALTA
Hardware	Hardware Tendes	70	0	17,5	17,5	80	2,5	7,2	ALTA
Hardware	Hardware Centre logístic	5	0	17,5	17,5	80	2,5	6	MITJA
Serveis	Servidors sscc i c.logistic	3	2,5	25	30	25	2,5	6,8	ALTA

Dades	Base de dades clients	120	25	45,25	32,5	30,25	10	9,6	ALTA
Dades	Base de dades productes	150	25	37,75	32,5	30,25	10	8,8	ALTA
Dades	Base de dades proveïdors	12	25	45,25	32,5	30,25	10	8,6	ALTA
Xarxa	Servidors botigues	2	12,5	20	40	75	10	7,8	ALTA
Aplicació	Software de facturació	19	12,5	37,5	37,5	45	7,5	9,6	ALTA
Xarxa	Xarxa de comunicació interna	3	12,5	20	40	75	10	7	ALTA
Equipament auxiliar	Serveis blindats de transport d'efectiu	2	0	40	15	100	0	7	ALTA
Equipament auxiliar	Flota de distribució	4	0	40	20	100	0	5,2	MTJA
Equipament auxiliar	Flota d'entrega	5	0	40	20	100	0	3,2	BAIXA
Equipament auxiliar	Flota comercials	3	0	40	20	100	0	2	BAIXA
Dades	Dades alumnes escoles	70	7,5	45,25	10	15,25	5	7,2	ALTA
Aplicació	Material de venta	30	5	15	15	40	2,5	5,2	MITJA
Aplicació	Material empleats	70	5	15	15	40	2,5	0,4	BAIXA
Hardware	Maquinària automatitzada de magatzem	2	0	17,5	17,5	80	2,5	3,2	BAIXA
Xarxa	Servidors de correu	7	15	42,5	40	47,5	20	4,2	MITJA
Instal·lacions	Instalacions SSCC	2	0	57,5	37,5	100	0	3,6	BAIXA
Instal·lacions	Instalacions centre logístic	3	0	57,5	37,5	100	0	3,8	BAIXA
Instal·lacions	Tendes	3	0	57,5	37,5	100	0	6,4	ALTA
Dades	Dades econòmiques i contables	1	25	35,25	7,5	35,25	5	6	MITJA
Personal	Treballadors	70	0	0	0	32,5	0	6,2	ALTA
Xarxa	Informació de xarxes socials	1	12,5	7,5	15	22,5	7,5	1,8	BAIXA
Aplicació	Perfil de xarxes socials	1	32,5	0	0	32,5	0	1,2	BAIXA
Instal·lacions	Material/mobiliari d'oficina/tenda	45	0	0	50	100	0	0,4	BAIXA

Instal·lacions	Arxiu documental fisic	3	0	57,5	37,5	100	0	4,8	MITJA
Dades	Arxiu docmental lògic	10	25	35,25	27,5	35,25	5	5,8	MITJA
Personal	Contractes de treballadors	0	2,5	15,25	7,5	10,25	5	6,2	ALTA
Aplicació	Documentació de normativa i estructuració interna	0	0	40	0	40	0	5,8	MITJA
Dades	Documentació productes pròpis	3	0	0	0	40	0	4	MITJA
Dades	Documentació confidencial de dades de negoci	0	0	40	0	40	0	6,4	MITJA
Serveis	Subministre electric	4	2,5	22,5	27,5	72,5	2,5	2,8	BAIXA
Serveis	Subministre d'internet i telefon	15	2,5	25	30	72,5	2,5	2,8	BAIXA
Serveis	Subministre aigua	3	2,5	22,5	27,5	72,5	2,5	1,6	BAIXA
Equipament auxiliar	Sistemes de seguretat (tendes i altres edificis)	1	0	40	25	100	25	8	MITJA

6.6 Determinació del nivell de risc acceptable i el risc residual

És necessari definir un límit a partir del qual podem decidir si assumir un risc o per el contrari no assumir-lo i, per tant, aplicar o no els controls definits. Aquest límit ha d'estar aprovat per la Direcció de l'empresa i s'han de definir els criteris per a establir-lo. Un cop establert el control per tal de reduir el risc, aquest actiu continuarà veient-

se exposat a un risc, però en aquest cas, reduït en comparació a l'estat inicial del risc, aquest risc resultant es l'anomenat risc residual.

En el nostre cas s'ha determinat amb la direcció que el risc acceptable es tot aquell actiu el valor del impacte del qual sigui inferior a ALTA. Per tant, en relació al risc que l'empresa considera acceptable es pren com apunt de referència el càlcul de l'impacte realitzat en l'apartat anterior d'aquest projecte.

Partint del nivell de risc determinat amb la direcció com a acceptable es realitzaran un seguit de controls (definits a continuació) sobre els recursos de l'empresa que estiguin amb una classificació de d'impacte superior o igual a ALTA, és adir, aquells que tenen un risc més alt i, per tant, que l'organització vol mitigar. Els principals actius que es tractaran són els següents:

Àmbit	Actiu	Valoració Impacte
Dades	Dades de clients	ALTA
Dades	Dades de proveïdors	ALTA
Dades	Informació personal empleats	ALTA
Aplicació	Software Web	ALTA
Aplicació	Software App	ALTA
Aplicació	Software terminals	ALTA
Hardware	Hardware SSCC	ALTA
Hardware	Hardware Tendes	ALTA
Serveis	Servidors sscc i c.logistic	ALTA
Dades	Base de dades clients	ALTA

Àmbit	Actiu	Valoració Impacte
Dades	Base de dades productes	ALTA
Dades	Base de dades proveïdors	ALTA
Xarxa	Servidors botigues	ALTA
Aplicació	Software de facturació	ALTA
Xarxa	Xarxa de comunicació interna	ALTA
Equipament auxiliar	Serveis blindats de transport d'efectiu	ALTA
Dades	Dades alumnes escoles	ALTA
Instal·lacions	Tendes	ALTA
Personal	Treballadors	ALTA
Personal	Contractes de treballadors	ALTA

Per a cadascun dels actius seleccionats es tractaran els riscos amb més probabilitat d'afectar-los i que suposen una criticitat major (descrits en l'apartat d'amenaces d'aquest document).

7. Propostes de projectes

7.1 Introducció

Amb el coneixement del nivell de risc actual de l'organització ha arribat el moment de plantejar els següents projectes per a la millora de l'estat de la seguretat de l'empresa.

Aquestes propostes de projectes estan destinades a mitigar el risc actual de l'organització i evolucionar el nivell ISO fins al nivell adequat, derivant-los dels resultats obtinguts en l'anàlisi de risc anterior basant-nos en les recomanacions associades a les amenaces identificades. Per tant, aquest projectes són el resultat d'agrupar les recomanacions identificades en la fase d'anàlisi de riscos. Es pretén incidir en la millora en relació a la gestió de la seguretat i en els beneficis qie aquests poden suposar sobre els recursos en general.

7.2 Objectiu

Aquestes propostes, per tant, tenen com a objectiu minimitzar els riscos identificats a un nivell acceptable per a l'empresa, contribuir en el desenvolupament de l'empresa a partir de les millores que es proposen, assegurar un futur de negoci per a l'empresa davant la materialització de possibles amenaces i facilitar les eines que permetin conèixer i identificar el nivell de seguretat de la informació de l'empresa.

7.3 Abast

Els projectes son el resultat del càlcul del risc de l'empresa i es dirigeixen a detectar i resoldre els punts febles i les vulnerabilitats dels controls. Aquests controls i projectes estan enfocats als actius de l'empresa, suposant una materialització d'un risc que suposi una pèrdua de recursos (econòmics, de personal, operatius, reputacionals, etc) per a la companyia XXXX.

7.4 Proposta de projectes

A continuació es mostren els projectes proposats per l'empresa analitzada en aquest projecte, dividint-los i classificant-los en base als 4 tipus de riscos sobre els que hem realitzat l'anàlisi, és adir, D'origen Industrial (OI), Desastres Natural (DN), d'origen Voluntari o atacs intencionats (AI) i errors o fallades no intencionades (NI).

7.4.1 Mitigació de riscos originats per desastres naturals o industrials

7.4.1.1 Objectiu

Amb aquest projecte es persegueix enfortir i disposar de mesures de prevenció sobre la seguretat ambiental els locals, edificis, flota de vehicles i actius dels incidents, d'aquesta forma es pretén no només reduir els riscos si no establir o millorar el tarannà de l'empresa en eficiència, consciencia de medi ambient i bones pràctiques. Per aconseguir-ho s'enfortiran els controls de seguretat física i ambiental de totes les instal·lacions físiques (que contenen la resta d'actius) i a més causar un impacte positiu en la cultura de l'empresa en matèries de riscos i pràctiques de conscienciació, economització i gestió eco-responsable.

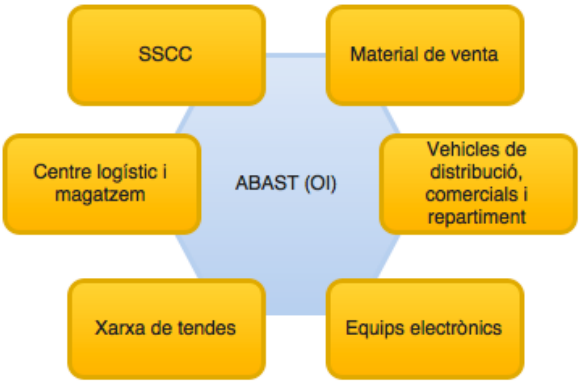
Un cop finalitzat i implementat el projecte l'organització podrà gestionar els incidents de forma directa i disposar dels avisos i les dades suficients per anticipar-s'hi; i poder reaccionar així ràpid davant d'inundacions, incendis, tempestes elèctriques, terratrèmols, excessos d'humitat o calor que puguin fer malbé actius o instal·lacions. A més, l'empresa serà capaç de tenir definits tasques de manteniment, seguiment i control dels dispositius encarregats d'assegurar la prevenció i anticipació a aquests riscos i, en cas de que fos necessari, poder regular-los i/o substituir-los.

Per altra banda cop a punt primordial, la validació i , en cas d'absència, la contractació d'assegurances i cobertures per tal d'assegurar que en cas de materialitzar-se alguna catàstrofe natural no perdre una quantia econòmica/material que suposi la caiguda de l'empresa. En cas de existir les cobertures adients, s'hauran de revisar i validar les

cobertures i costos d'aquestes per tal d'assegurar una optima protecció de l'organització. Per acabar, l'organització serà capaç de mantenir una plantilla informada, formada i llesta per a afrontar, prevenir i conscienciar en matèries de prevenció d'incidents d'aquesta mena i en gestió eficient dels dispositius que regulen aspectes tant importants com el clima, les deixalles, etc.

7.4.1.2 Abast

L'abast d'aquest projecte de millora de la seguretat davant riscos d'origen natural avarca totes les instal·lacions físiques i actius citats en l'esquema següent:



7.4.1.3 Tasques a realitzar

Per a la implementació del projecte s'hauran de duu a terme un seguit d'accions distribuïdes en les següents fases:

1. Recopilació d'informació de controls, equips, procediments de la companyia en matèria de pretensió de desastres naturals.
2. Determinació de la normativa vigent i legislació en el territori espanyol referent al tractament i gestió de riscos d'aquesta classe.
3. Recopilació, anàlisi i conclusions dels incidents que hagin pogut succeir en aquest àmbit a l'empresa, i les actuacions executades per a resoldre-les.
4. Contactar i contractar a terceres empreses de serveis que proporcionin instal·lacions, material, assegurances i altres serveis necessaris per a establir les salvaguardes i avisos necessaris. En aquest cas, de tot aquell servei o contracte

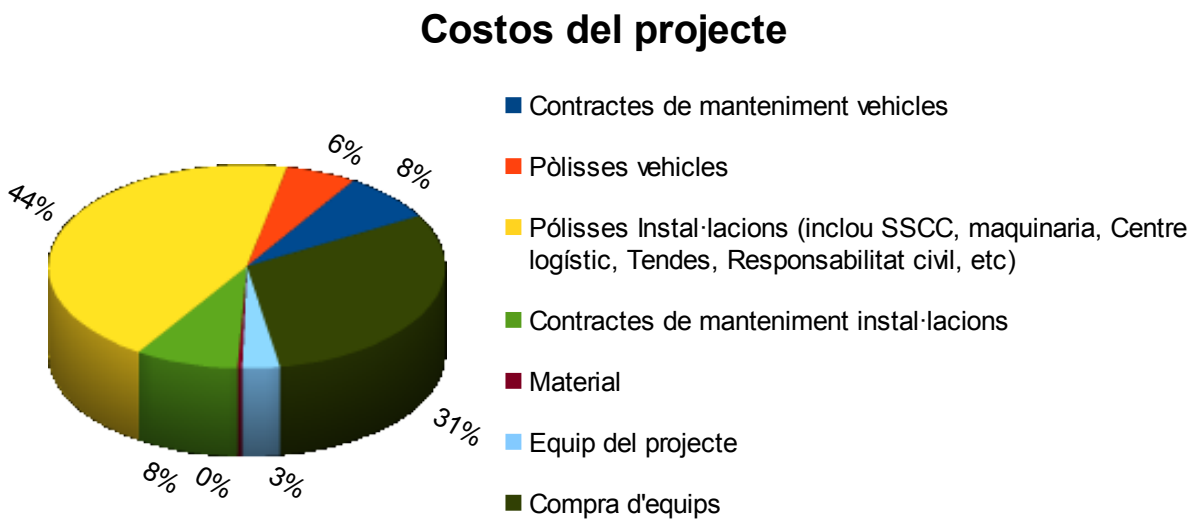
que es disposi instaurat actualment, es tindrà que considerar i jutjar si les cobertures, prestacions i serveis són els adequats per tal de satisfer l'objectiu perseguit (tant a nivell econòmic com pràctic). Es vol protegir contra incendi, inundacions, fallades elèctriques, danys d'equips per fallades elèctriques aigua o foc, trencaments accidentals, destrucció, robatoris, etc.

5. Redacció i disseny de protocols, estratègies, plans, instal·lacions d'equips i dispositius necessaris per a poder monitoritzar, mantenir, gestionar i reaccionar més ràpidament davant de riscos d'aquest tipus.
6. Fase de proves i simulacres, per tal de determinar el grau de maduresa dels mecanismes i dispositius i la seva eficiència i eficàcia. Per a fer-ho es dissenyaran escenaris de proves i es determinaran dates (no informades al personal en segons quins casos) per a simular incidents i poder avaluar la reacció dels empleats per tal de poder millorar la seva actuació en aquests casos.
7. Formació i conscienciació del personal, establint responsables en els departaments i a recursos humans per tal de gestionar una formació activa, anualitzada i correcta.
8. Posada en marxa dels elements provats i validats i posada a disposició de la direcció de la companyia.

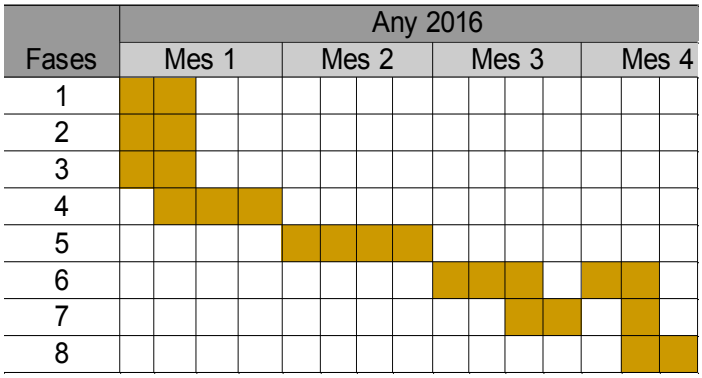
7.4.1.4 Recursos i temporalitat

Pel que fa als costos del projecte, s'han quantificat en base al pressupost que s'ha estimat que podria ser necessari destinar-hi. A continuació es poden observar els costos referents als honoraris dels membres que hauran d'implantar el projecte, material, dietes/desplaçaments, equips, instal·lacions i altres serveis necessaris.

Contractes de manteniment vehicles	20000
Pòlisses vehicles	15000
Pólisses Instal·lacions (inclou SSCC, maquinaria, Centre logístic, Tendes, Responsabilitat civil, etc)	115000
Contractes de manteniment instal·lacions	22000
Material	400
Equip del projecte	8000
Compra d'equips	80000
cost total del projecte (€)	260400



El “time-line”, o cronograma del projecte, seria el següent (suposant un projecte d'un any):



7.4.1.5 Riscos a mitigar

Amb l'aplicació d'aquest projecte es persegueix mitigar els riscos derivats d'accions natural o industrials. Aquests poden ser diversos, per això s'han agrupat segons l'origen en la següent taula, on es mostren un exemple de cadascun dels riscos que s'ha perseguit mitigar, evitar o millorar la resposta o compensació per pèrdues de l'empresa davant d'aquests.

- Foc, per exemple incendis en instal·lacions causats per fallades elèctriques, derivades per exemple de llamps o mal estat del cablejat de les instal·lacions.
- Temperatura elevada o baixa, com per exemple glaçades o danys a actius de venta per deteriorament degut als rajos solars.
- Danys per aigua, en casos d'inundacions, goteres, filtracions, que puguin danyar equips informàtics, vehicles, etc.
- Variacions en condicions d'humitat, per exemple afectació de servidors o altres dispositius elèctrics o material de papereria.
- La degradació dels suports d'emmagatzematge, per exemple la destrucció de discs durs amb informació important d'empresa dels quals no es tingui copia.
- Contaminació mecànica i electromagnètica, que per exemple poden danyar els actius electrònics i sistemes de venta.
- Averies físiques o lògiques, per exemple degudes a fallades de serveis aliens a l'empresa com podrien ser punxades de pneumàtics o pèrdues en malbaratament de subministres (fugues, trencades, embossaments, mal estat elèctric).
- Talls de subministres, per exemple caigudes de la xarxa elèctrica.

7.4.1.6 Controls afectats

Amb l'aplicació d'aquest projecte en l'SGSI de l'empresa es pretén afectar positivament als següents controls definits per la norma ISO:

5.POLÍTICA DE SEGURIDAD.
- **5.1 Política de seguridad de la información.**
  - **5.1.1 Documento de política de seguridad de la información.**
  - **5.1.2 Revisión de la política de seguridad de la información.**

6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- **6.1 Organización interna.**
  - **6.1.1 Compromiso de la Dirección con la seguridad de la información.**
  - **6.1.2 Coordinación de la seguridad de la información.**
  - **6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.**
  - **6.1.4 Proceso de autorización de recursos para el tratamiento de la información.**
  - **6.1.5 Acuerdos de confidencialidad.**
  - **6.1.6 Contacto con las autoridades.**
  - **6.1.7 Contacto con grupos de especial interés.**
  - **6.1.8 Revisión independiente de la seguridad de la información.**
- **6.2 Terceros.**
  - **6.2.1 Identificación de los riesgos derivados del acceso de terceros.**
  - **6.2.2 Tratamiento de la seguridad en la relación con los clientes.**
  - **6.2.3 Tratamiento de la seguridad en contratos con terceros.**
  - **7.1.3 Uso aceptable de los activos.**
  - **8.2.1 Responsabilidades de la Dirección.**
  - **8.2.2 Concienciación, formación y capacitación en seg. de la informac.**
  - **9.1.4 Protección contra las amenazas externas y de origen ambiental.**
- **9.2 Seguridad de los equipos.**
  - **9.2.1 Emplazamiento y protección de equipos**
  - **9.2.2 Instalaciones de suministro.**
  - **9.2.3 Seguridad del cableado.**
  - **9.2.4 Mantenimiento de los equipos.**
  - **9.2.5 Seguridad de los equipos fuera de las instalaciones.**
  - **9.2.7 Retirada de materiales propiedad de la empresa.**
- **10.2 Gestión de la provisión de servicios por terceros.**
  - **10.2.1 Provisión de servicios.**
  - **10.2.2 Supervisión y revisión de los servicios prestados por terceros.**
  - **10.2.3 Gestión del cambio en los servicios prestados por terceros.**
- **10.10 Supervisión.**
  - **10.10.1 Registros de auditoría.**
  - **10.10.2 Supervisión del uso del sistema.**
  - **10.10.3 Protección de la información de los registros.**
  - **10.10.4 Registros de administración y operación.**
  - **10.10.5 Registro de fallos.**

13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- **13.1 Notificación de eventos y puntos débiles de seguridad de la información.**
  - **13.1.1 Notificación de los eventos de seguridad de la información.**
  - **13.1.2 Notificación de puntos débiles de seguridad.**
- **13.2 Gestión de incidentes y mejoras de seguridad de la información.**
  - **13.2.1 Responsabilidades y procedimientos.**
  - **13.2.2 Aprendizaje de los incidentes de seguridad de la información.**
  - **13.2.3 Recopilación de evidencias.**

14.GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- **14.1 Aspectos de seguridad de la información en la gestión de la continuidad del nego**
  - **14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la cor**
  - **14.1.2 Continuidad del negocio y evaluación de riesgos.**
  - **14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad**
  - **14.1.4 Marco de referencia para la planificación de la cont. del negocio.**
  - **14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.**

15.CUMPLIMIENTO.

7.4.2 Mitigació de riscos d'origen involuntari

7.4.2.1 Objectiu

Amb aquest projecte es persegueix enfortir i disposar de mesures de prevenció sobre la seguretat lògica i física (p.e.: xarxes, servidors, accessos a terminals, establiments, danys accidentals, etc) que puguin afectar a actius crítics de la companyia causats per errors del personal de l'empresa, els clients de l'empresa i els usuaris dels seus serveis. Un cop finalitzat i implementat el projecte l'organització veurà millorada la seva capacitat per a evitar els riscos, identificar-los i mitigar-los.

L'objectiu d'aquest projecte es aconseguir que la companyia pugui disposar de programari antivirus, tallafocs per tal d'evitar el mal ús d'aquesta (per descarrega de contingut maliciós per exemple, no intencionadament). Disposar d'un sistema d'alertes que ajudi a prevenir, evitar o avisar sobre els errors que es puguin produir tant a nivell hardware, software o d'accés físic a les instal·lacions. També es persegueix protegir els actius de venta al públic del deteriorament o trencades accidentals per part dels treballadors, tant a les tendes com als serveis logístics i centrals. Es persegueix poder millorar les condicions laborals dels treballadors en matèria de riscos laborals per minimitzar danys sobre els empleats i les instal·lacions i minimitzar baixes.

A més, al igual que en el projecte anterior, es dotarà, verificarà i/o validarà la cobertura a nivell assegurador de les pòlisses que disposi la companyia davant de pèrdues i dany d'equips. Tenir predefinida una política o estàndard d'actuació per als empleats per tal de poder pautar i fixar metodologies per a segons quines tasques. Per altra banda, s'implantarà un sistema de formació interna per tal de conèixer temes tals com els riscos laborals, prevenció de frau, habilitats de venta, etc. Per a evitar la fuga de dades i altra informació o material sensible es revisaran i establiran els controls i protocols per a manejar aquests actius.

En resum, amb aquest projecte es millorarà i enfortirà la seguretat física i lògica de la

cooperativa XXXX incrementant així la confiança i la valoració que els clients, proveïdors, socis, accionistes, empleats i usuaris tenen sobre aquesta en temes de prevenció de riscos i fallades accidentals.

7.4.2.2 Abast

L'abast d'aquest projecte de millora de la seguretat davant riscos d'origen in-intencionat avarca tots els actius físics i lògics següents:

Dades de clients
Dades de proveïdors
Factures
Tarifes i ofertes
Inventari
Dades econòmiques de les tendes
Informació personal empleats
Software Web
Software App
Software terminals
Hardware SSCC
Hardware Tendes
Hardware Centre logístic
Servidors sscc i c.logistic
Base de dades clients
Base de dades productes
Base de dades proveïdors
Servidors botigues
Software de facturació
Xarxa de comunicació interna
Serveis blindats de transport d'efectiu
Flota de distribució
Flota d'entrega
Flota comercials
Dades alumnes escoles
Material de venta
Material empleats
Maquinària automatitzada de magatzem
Servidors de correu
Instalacions SSCC
Instalacions centre logístic
Tendes
Dades econòmiques i contables
Treballadors
Informació de xarxes socials
Perfil de xarxes socials
Material/mobiliari d'oficina/tenda
Arxiu documental fisic
Arxiu docmental lògic
Contractes de treballadors
Documentació de normativa i estructuració interna
Documentació productes pròpis
Documentació confidencial de dades de negoci
Subministre electric
Subministre d'internet i telefon
Subministre aigua
Sistemes de seguretat (tendes i altres edificis)

7.4.2.3 Tasques a realitzar

Per a la implementació del projecte s'hauran de duu a terme un seguit d'accions distribuïdes en les següents fases:

1. Recopilació d'informació de controls, equips, procediments de la companyia.
2. Determinació de la normativa vigent i legislació en el territori espanyol referent al tractament i gestió de riscos laborals, sanitaris i serveis.
3. Recopilació, anàlisi i conclusions dels incidents que hagin pogut succeir en aquest àmbit a l'empresa, i les actuacions executades per a resoldre-les.
4. Contactar i contractar a terceres empreses de serveis que proporcionin instal·lacions, material, assegurances i altres serveis necessaris per a establir les salvaguardes i avisos necessaris. En aquest cas, de tot aquell servei o contracte que es disposi instaurat actualment, es tindrà que considerar i jutjar si les cobertures, prestacions i serveis són els adequats per tal de satisfer l'objectiu perseguit (tant a nivell econòmic com pràctic). Es persegueix protegir l'empresa contra robatori, atacs destructius i ocupació enemiga.
5. Redacció i disseny de protocols, estratègies, plans, instal·lacions d'equips i dispositius necessaris per a poder monitoritzar, mantenir, gestionar i reaccionar més ràpidament davant de riscos d'aquest tipus. En aquesta fase es dissenyaran els mecanismes de gestió de canvis, manteniment, registre d'events, entrenament del sistema, configuració del software i equips, mètriques de mesura, proves a realitzar sobre els equips, instal·lacions i software, tests de penetració de xarxa i avaluació dels proveïdors.
6. Fase de proves i simulacres, per tal de determinar el grau de maduresa dels mecanismes i dispositius i la seva eficiència i eficàcia. Per a fer-ho es dissenyaran escenaris de proves i s'executaran les proves i activitats determinades a la fase anterior i, així simular incidents i, poder avaluar la reacció dels mecanismes i sistemes implantats.
7. Formació i conscienciació del personal, establint responsables en els departaments i a recursos humans per tal de gestionar una formació activa, anual i correcta (en les matèries exposades en els objectius del segon paràgraf

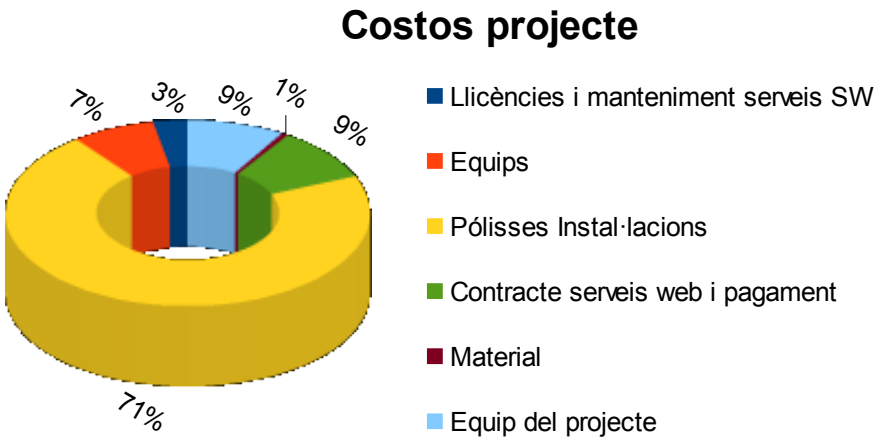
d'aquest projecte de millora de la seguretat).

8. Posada en marxa dels elements provats i validats i posada a disposició de la direcció de la companyia.

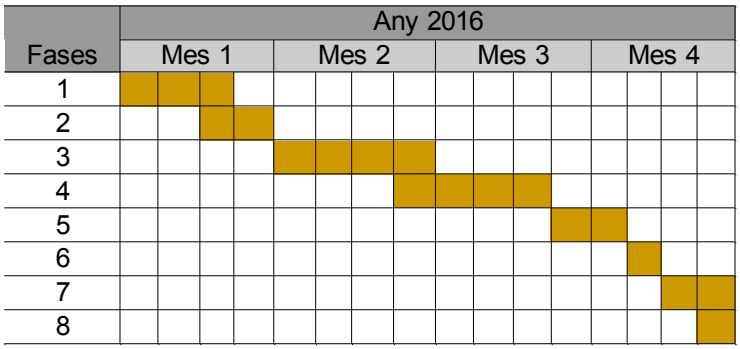
7.4.2.4 Recursos i temporalitat

Pel que fa als costos del projecte, s'han quantificat en base al pressupost que s'ha estimat que podria ser necessari destinar-hi. A continuació es poden observar els costos referents als honoraris dels membres que hauran d'implantar el projecte, material, dietes/desplaçaments, equips, instal·lacions i altres serveis necessaris.

Llicències i manteniment serveis SW	5000
Equips	12000
Pólisses Instal·lacions	115000
Contracte serveis web i pagament	15000
Material	1000
Equip del projecte	14000
cost total del projecte (€)	162000



El “time-line”, o cronograma del projecte, seria el següent:



7.4.2.5 Riscos a mitigar

Amb l'aplicació d'aquest projecte es persegueix mitigar els riscos derivats d'actuacions del personal de l'empresa fetes de forma no intencionada (o sense ànim de dol). Aquests poden ser diversos, per això s'han agrupat segons l'origen en la següent taula, on es mostren un exemple de cadascun dels riscos que s'ha perseguit mitigar, evitar o millorar la resposta o compensació per pèrdues de l'empresa davant d'aquests.

- Errors d'usuaris i d'administrador, per exemple errades en la introducció de codi o text en les aplicacions, causant així un error en un preu en el catàleg de productes de l'aplicació web.
- Errors de monitorització i configuració, per exemple una mala configuració del sistemes de retard de les caixes de les tendes que causen una aturada de la facturació a les primeres hores de la jornada de venta al públic.
- Deficiències de l'organització, per exemple errors de concepte i organització de les tasques, que són aliens als empleats per ser pre-definits pels protocols de l'empresa.
- Difusió de software perjudicial, errors de re-/encaminament i de seqüència, per exemple un empleat descarrega fitxers d'un origen poc segur o d'un correu electrònic enviat per a intentar atacar el sistema, sent l'empleat inconscient del perill del correu que esta visualitzant (com podria ser documentació adjunta executable).

- Fugues d'informació, per exemple mala destrucció o pèrdua accidental de documents interns.
- Alteracions accidentals d'informació o destrucció d'informació, per exemple un empleat elimina un fitxer del que no se n'havia realitzat còpia.
- Vulnerabilitats dels programes, per exemple degudes a fallades en l'arquitectura de la plataforma que s'està utilitzant per a programar-les.
- Errors de manteniment / actualització de programes o de hardware, per exemple la no actualització d'un equip provoca que un software maliciós exploti una vulnerabilitat que en la versió actualitzada no hi esta present o multes, tallades de servei o exposició dels equips davant de la no actualització (mitjançant pagament de llicències) del software llicenciat.
- Caigudes del sistema causades per esgotament de recursos, pèrdua d'equips i in-disponibilitat del personal, per exemple trencament per ús irresponsable o inconscient d'un monitor dels terminals d'oficines o malalties d'empleats.

7.4.2.6 Controls afectats

Amb l'aplicació d'aquest projecte en l'SGSI de l'empresa es pretén afectar positivament als següents controls definits per la norma ISO:

5.POLÍTICA DE SEGURIDAD.
- **5.1 Política de seguridad de la información.**
  - **5.1.1 Documento de política de seguridad de la información.**
  - **5.1.2 Revisión de la política de seguridad de la información.**

6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- **6.1 Organización interna.**
  - **6.1.1 Compromiso de la Dirección con la seguridad de la información.**
  - **6.1.2 Coordinación de la seguridad de la información.**
  - **6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.**
  - **6.1.4 Proceso de autorización de recursos para el tratamiento de la información.**
  - **6.1.5 Acuerdos de confidencialidad.**
  - **6.1.6 Contacto con las autoridades.**
  - **6.1.7 Contacto con grupos de especial interés.**
  - **6.1.8 Revisión independiente de la seguridad de la información.**
- **6.2 Terceros.**
  - **6.2.1 Identificación de los riesgos derivados del acceso de terceros.**
  - **6.2.2 Tratamiento de la seguridad en la relación con los clientes.**
  - **6.2.3 Tratamiento de la seguridad en contratos con terceros.**

7.GESTIÓN DE ACTIVOS.
- **7.1 Responsabilidad sobre los activos.**
  - **7.1.1 Inventario de activos.**
  - **7.1.2 Propiedad de los activos.**
  - **7.1.3 Uso aceptable de los activos.**
- **7.2 Clasificación de la información.**
  - **7.2.1 Directrices de clasificación.**
  - **7.2.2 Etiquetado y manipulado de la información.**

8.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- **8.1 Antes del empleo.**
  - **8.1.1 Funciones y responsabilidades.**
  - **8.1.2 Investigación de antecedentes.**
  - **8.1.3 Términos y condiciones de contratación.**
- **8.2 Durante el empleo.**
  - **8.2.1 Responsabilidades de la Dirección.**
  - **8.2.2 Concienciación, formación y capacitación en seg. de la informac.**
  - **8.2.3 Proceso disciplinario.**
- **8.3 Cese del empleo o cambio de puesto de trabajo.**
  - **8.3.1 Responsabilidad del cese o cambio.**
  - **8.3.2 Devolución de activos.**
  - **8.3.3 Retirada de los derechos de acceso.**

9.SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1.2 Controles físicos de entrada.

9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos

9.2.4 Mantenimiento de los equipos.

9.2.5 Seguridad de los equipos fuera de las instalaciones.

9.2.6 Reutilización o retirada segura de equipos.

9.2.7 Retirada de materiales propiedad de la empresa.

10.GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.

10.1.2 Gestión de cambios.

10.1.3 Segregación de tareas.

10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

10.2.1 Provisión de servicios.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

10.3.1 Gestión de capacidades.

10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

10.4.1 Controles contra el código malicioso.

10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

10.7.1 Gestión de soportes extraíbles.

10.7.2 Retirada de soportes.

10.7.3 Procedimientos de manipulación de la información.

10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

10.8.2 Acuerdos de intercambio.

10.8.3 Soportes físicos en tránsito.

10.8.4 Mensajería electrónica.

10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
11.CONTROL DE ACCESO.
11.3 Responsabilidades de usuario.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.4 Seguridad de los archivos de sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.

7.4.3 Mitigació de riscos d'origen atacs intencionats

7.4.3.1 Objectiu

Amb aquest projecte es persegueix enfortir i disposar de mesures i controls per a prevenir, actuar i afrontar atacs i altres accions intencionades que persegueixin malmetre els actius físics, lògics i reputacionals de l'empresa XXXXX, ja siguin d'origen intern a l'organització, com per exemple personal en plantilla, com personal extern a aquesta, com per exemple ex-empleats, la competència o clients. Un cop finalitzat i implementat el projecte l'organització veurà millorada la seva capacitat per a evitar els riscos, identificar-los i minimitzar el seu impacte.

Amb aquest projecte es millorarà i enfortirà la seguretat física i lògica de la cooperativa XXXX incrementant així la confiança i la valoració que els clients, proveïdors, socis, accionistes, empleats i usuaris tenen sobre aquesta en temes de protecció i seguretat davant d'atacs, delictes i altres accions lesives intencionades.

L'objectiu d'aquest projecte es aconseguir que l'empresa aconsegueixi disposar d'un sistema de monitorització i control de l'activitat, tràfic i ús de tots els actius, àrees i zones restringides que pugessin malmetre greument el futur del negoci, la reputació de l'empresa o l'activitat de negoci diària.

Al igual que amb la resta de projectes, l'empresa disposarà de les pòlisses necessàries per a poder afrontar tant indemnitzacions, substitucions, recursos mèdics i compensacions econòmiques, davant d'actes que siguin lesius per a l'empresa, els seus actius i els seus treballadors.

Per altra banda es disposarà de personal format i conscienciat en termes de prevenció d'atacs, conflictes i altres successos que poguessin afectar en aquesta àrea en funció del seu lloc de treball. Per últim es persegueix tenir establerts uns protocols, bones pràctiques i configuracions en els equips que permetin minimitzar les intrusions i danys

d'aquest tipus.

7.4.3.2 Abast

L'abast d'aquest projecte de millora de la seguretat davant riscos d'origen in-intencionat avarca tots els actius físics i lògics següents:

Dades de clients	Dades alumnes escoles
Dades de proveïdors	Material de venta
Factures	Material empleats
Tarifes i ofertes	Maquinària automatitzada de magatzem
Inventari	Servidors de correu
Dades econòmiques de les tendes	Instalacions SSCC
Informació personal empleats	Instalacions centre logístic
Software Web	Tendes
Software App	Dades econòmiques i contables
Software terminals	Treballadors
Hardware SSCC	Informació de xarxes socials
Hardware Tendes	Perfil de xarxes socials
Hardware Centre logístic	Material/mobiliari d'oficina/tenda
Servidors sscc i c.logistic	Arxiu documental fisic
Base de dades clients	Arxiu docmental lògic
Base de dades productes	Contractes de treballadors
Base de dades proveïdors	Documentació de normativa i estructuració interna
Servidors botigues	Documentació productes pròpis
Software de facturació	Documentació confidencial de dades de negoci
Xarxa de comunicació interna	Subministre d'internet i telefon
Serveis blindats de transport d'efectiu	Sistemes de seguretat (tendes i altres edificis)
Flota de distribució	Flota comercials
Flota d'entrega	

7.4.3.3 Tasques a realitzar

Per a la implementació del projecte s'hauran de duu a terme un seguit d'accions distribuïdes en les següents fases:

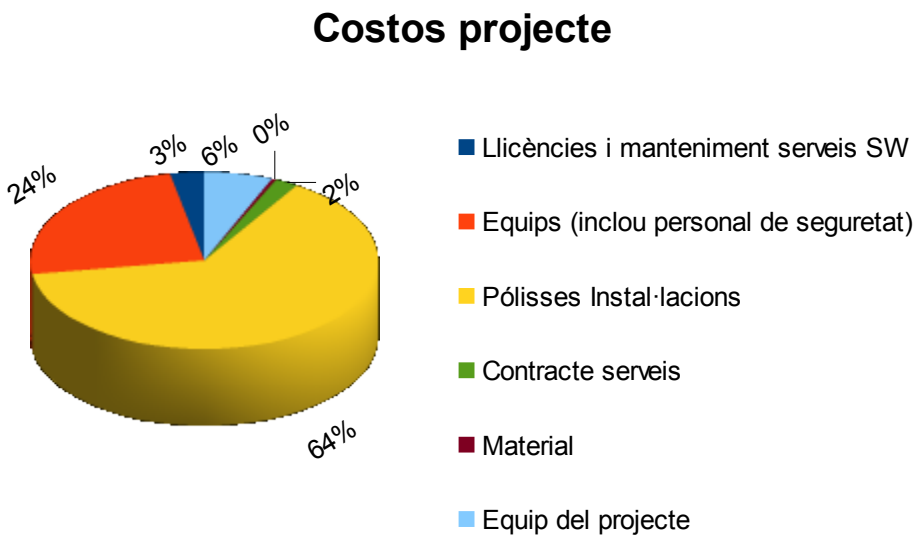
1. Recopilació d'informació de controls, equips, procediments de la companyia.
2. Determinació de la normativa vigent i legislació en el territori espanyol referent al tractament i gestió de delictes, atacs, denegacions de servei de subministres o serveis informàtics, etc.
3. Recopilació, anàlisi i conclusions dels incidents que hagin pogut succeir en aquest àmbit a l'empresa, i les actuacions executades per a resoldre-les.

4. Contactar i contractar a terceres empreses de serveis que proporcionin instal·lacions, material, assegurances, serveis jurídics i legals, forces de seguretat per a establir les salvaguardes, mecanismes d'avís o defensa legal i avisos necessaris per a afrontar els incidents amb suficient rapidesa i legalitat com sigui possible. En aquest cas, de tot aquell servei o contracte que es disposi instaurat actualment, es tindrà que considerar i jutjar si les cobertures, prestacions i serveis són els adequats per tal de satisfer l'objectiu perseguit (tant a nivell econòmic com pràctic). Es persegueix protegir l'empresa contra robatori, atacs destructius, lesions a empleats, lesions a col·laboradors, lesions a clients, vandalisme i ocupació enemiga.
5. Redacció i disseny de protocols, estratègies, plans, polítiques, instal·lacions d'equips i dispositius necessaris per a poder monitoritzar, mantenir, gestionar i reaccionar més ràpidament davant de riscos d'aquest tipus, tant a nivell de Software, Hardware, d'instal·lacions i plans d'actuació i formació. En aquesta fase es dissenyaran els procediments, manteniments, mètodes d'enregistrament d'events, configuració d'equips i tecnologies, escenaris de proves i contractes necessaris.
6. Fase de proves i simulacres, per tal de determinar el grau de maduresa dels mecanismes i dispositius i la seva eficiència i eficàcia. Per a fer-ho es dissenyaran escenaris de proves i s'executaran les proves i activitats determinades a la fase anterior i, així simular incidents i, poder avaluar la reacció dels mecanismes i sistemes implantats, per a poder comprovar que estan correctament dissenyats i implantats.
7. Formació i conscienciació del personal, establint responsables en els departaments i a recursos humans per tal de gestionar una formació activa, actualitzada i correcta (en les matèries exposades en els objectius d'aquest projecte de millora de la seguretat).
8. Posada en marxa dels elements provats i validats i posada a disposició de la direcció de la companyia.

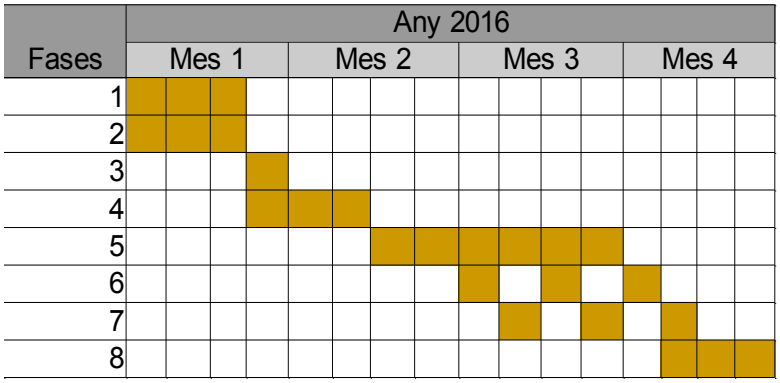
7.4.3.4 Recursos i temporalitat

Pel que fa als costos del projecte, s'han quantificat en base al pressupost que s'ha estimat que podria ser necessari destinar-hi. A continuació es poden observar els costos referents als honoraris dels membres que hauran d'implantar el projecte, material, dietes/desplaçaments, equips, instal·lacions i altres serveis necessaris.

Llicències i manteniment serveis SW	3000
Equips (inclou personal de seguretat)	23000
Pólisses Instal·lacions	60000
Contracte serveis	2000
Material	400
Equip del projecte	6000
cost total del projecte (€)	94400



El “time-line”, o cronograma del projecte, seria el següent:



7.4.3.5 Riscos a mitigar

Amb l'aplicació d'aquest projecte es persegueix mitigar els riscos derivats d'accions de personal extern o intern que vulgui afectar al funcionament o apropiar-se de recursos o actius de l'empresa de forma intencionada. Aquests poden ser diversos, per això s'han agrupat segons l'origen en la següent taula, on es mostren un exemple de cadascun dels riscos que s'ha perseguit mitigar, evitar o millorar la resposta o compensació per pèrdues de l'empresa davant d'aquests.

- Suplantació d'identitat d'usuari o accés no autoritzat, per exemple un agent extern que accedeixi a àrees segures de l'empresa amb identificació de contrasenya i noms d'usuari d'un empleat que havia apuntat les seves credencials en un paper.
- Manipulació configuració o logs del sistema, per exemple un usuari intern que canvií la configuració de les alarmes per a poder ajudar a que algú extern accedeixi a les instal·lacions.
- Abús de privilegis d'accés i ús no previst, per exemple usuaris que accedeixin a informació confidencial a la que hi tenen accés per a poder filtrar informació per lucrar-se amb la competència.
- Difusió de software maliciós, per exemple un ex-empleat que utilitzi les seves antigues credencials i coneixements del sistema per a introduir software que aturi la plataforma de pagament o desviï ingressos a altres persones.
- Re-/encaminament missatges, per exemple un agent extern que mitjançant

l'accés a la xarxa de correu desviï copies de totes les comunicacions internes per a finalitats pròpies i lucratives.

- Alteració de seqüencies i anàlisis de tràfic, originat per exemple per un usuari extern a la xarxa que analitza les comunicacions i el tràfic de l'empresa per a filtrar informació a tercers.
- Modificació d'informació, intercepció d'informació, destrucció d'informació i divulgació d'informació, per exemple per a poder vendre a la competència informació privilegiada de negoci.
- Manipulació d'equips i programes, per exemple per deixar sense plataforma de pagament a les tendes.
- Denegació de servei, per exemple una empresa proveïdora de serveis d'internet o telecomunicacions que decideixi tallar el subministrament sense raons.
- Robatoris, atac destructiu o ocupació enemiga, per exemple un grup d'individus externs prenen una tenda per a robar, i malmetre als empleats, actius i estoc d'aquesta.
- In-disponibilitat del personal, per exemple, baixes no justificades d'empleats.
- Extorsió, per exemple davant d'ex-empleat que amenacin a l'empresa en vendre secrets d'aquesta a la competència a canvi de compensacions econòmiques o tractes preferents

7.4.3.6 Controls afectats

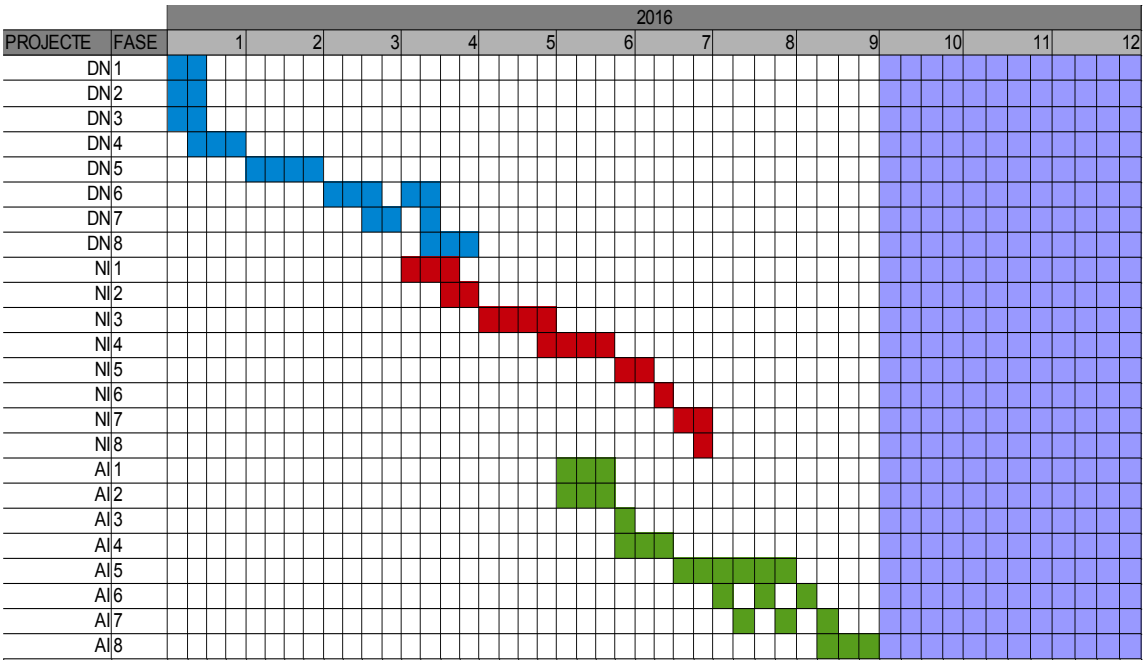
Amb l'aplicació d'aquest projecte en l'SGSI de l'empresa es pretén afectar positivament a tots els controls definits per la norma, ja que qualsevol materialització d'amenaces en aquest aspecte afecta directa o indirectament a tots els controls definits (per a veure un llistat de tots els controls definits per la norma ISO, consultar annex A.E).

7.5 Planificació temporal

En l'annex B.E, apartat Planificació, es poden observar les taules de planificació de la implantació de cada projecte i la planificació global.

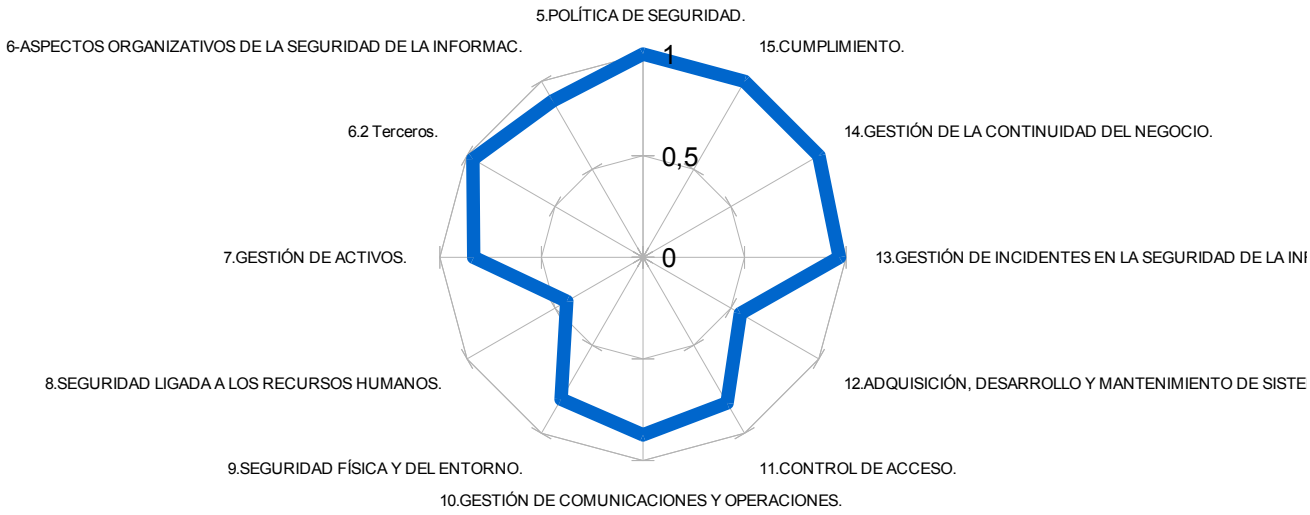
En aquests s'ha pres com a consideració el límit temporal per a planificar tot el procés d'implantació 1 any, del qual es pot observar que l'últim trimestre es correspondria a la avaluació, control i presa de decisions de la direcció i organismes pertinents de l'empresa per a poder planificar les següent iteracions de millora i avaluació del sistema, per als objectius que l'empresa es proposa per l'anualitat posterior.

En la següent taula es pot observar la planificació de les diferents fases dels tres projectes (observar que els projectes s'0han referenciat en funció de si són DN = desastres naturals i origen industrial, NI = No intencionats, AI = Atacs intencionats).



7.6 Estimació del compliment de la norma

Un cop definits els projectes el següent pas es aproximar el càlcul de com es veuria repercutit l'impacte dels riscos i la freqüència d'ocurrència d'aquests; per això, en la següent taula, es poden veure l'evolució dels diferents dominis definits per la norma ISO/IEC 27002, ja que com a resultat de l'aplicació dels projectes, les probabilitats de materialització del risc i la seguretat dels actius en cada dimensió s'hauran vist afectades positivament. Com es pot observar en gràfic de radar següent, les àrees mes afectades positivament pels canvis son les que estan directament implicades amb les polítiques de seguretat, documentació, definició de protocols de control de la seguretat i en les que hi serien més presents els actius definits en el punt anterior d'aquest projecte. En l'annex B.E es poden observar les taules dels controls en el punt previ al projecte i un cop aplicats els projectes, que donen forma al gràfic següent.



8. Auditoria de compliment

8.1 Anàlisi de resultats i constatacions

Arribats en aquest punt, amb el coneixement dels actius, negoci i riscos de l'empresa i un cop analitzades les amenaces, podem determinar fins a quin punt l'empresa compleix les “bones pràctiques” en matèria de seguretat. Aquestes “bones pràctiques” venen definides per la norma ISO/IEC 27002:2013, ja que descriu un marc de control de l'estat de la seguretat del sistema. Aquesta norma, que es tracta d'un estàndard internacionalment reconegut i vàlid per a la majoria d'organitzacions, agrupa 113 controls i/o mesures preventives per a la gestió de la seguretat de la informació, organitzant-se en 14 àrees i 35 objectius de control.

Per a realitzar aquesta avaluació de la maduresa de la seguretat en la nostra organització serà necessari l'elaboració d'un informe d'auditoria, tenint en compte que els projectes anteriorment definits s'han implementat. Per a poder realitzar la valoració de la maduresa esmentada es prendrà per referència la llegenda següent (basada en el CMM, model de maduresa de la capacitat).

Nivell	Percentatge	Descripció
Inexistent	0,00%	Absència completa de qualsevol procés. No es reconeix que hi ha un problema que resoldre. Absència de completa de qualsevol procés.
Inicial /Ad-hoc	10,00%	Estat inicial on l'èxit de les activitats dels processos es basa en l'esforç personal, la majoria de les vegades. Els procediments son inexistents o localitzats en àrees concretes. No existeixen plantilles definides a nivell corporatiu.
Reproduïble, però intuïtiu	50,00%	Els processos similars es gestionen de forma similar per diferents persones amb la mateixa tasca. Es normalitzen les bones pràctiques en base a l'experiència i al mètode. No hi ha comunicació o entrenament formal, les responsabilitats es queden a càrrec de cada

		individu. Dependència del grau de coneixement de cada individu.
Procés definit	90,00%	L'organització sencera participa en el procés. Els processos estan implantats, documentats i comunicats mitjançant entrenament formal.
Gestionat i mesurable	95,00%	Es pot prosseguir amb indicadors numèrics i estadístics la evolució dels processos. Es disposa de tecnologia per autoritzar el flux de treball i es disposa d'eines de millora de la qualitat i la eficiència.
Optimitzat	100,00%	Els processos estan sota constant millora. Es determinen les desviacions i s'optimitzen els processos en base a criteris quantitatius.

En l'annex A.P es pot observar la relació d'objectius de control dels dominis definits per la norma per a l'estat esperat de la seguretat del SGSI un cop implantats els projectes esmentats en l'apartat anterior. Per a fer-ho es calcularà la mitja dels nivells de compliments de cada control, obtenint així el nivell de compliment en relació als objectius de control.

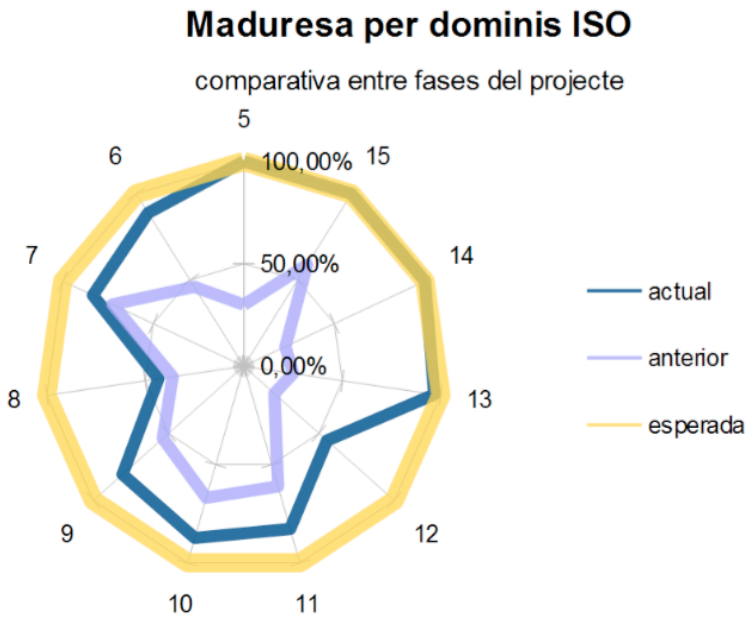
En la següent taula es poden apreciar per a cada control els percentatges de maduresa un cop implementats els projectes:

ACTUAL – POST PROJECTES	
5.POLÍTICA DE SEGURIDAD.	100,00%
6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	88,90%
7.GESTIÓN DE ACTIVOS.	83,33%
8.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	43,33%
9.SEGURIDAD FÍSICA Y DEL ENTORNO.	80,60%
10.GESTIÓN DE COMUNICACIONES Y OPERACIONES.	87,36%
11.CONTROL DE ACCESO.	82,75%
12.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	55,36%
13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	96,67%
14.GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	100,00%
15.CUMPLIMIENTO.	100,00%

En la següent taula es poden observar, per a cada nivell definit la proporció de controls que s'hi comprenen:

ESTAT PER NIVELLS DE MADURESA		
inexistent	1	1%
adhoc	22	14%
reproduible	53	33%
definit	25	15%
gestionat	20	12%
optimitzat	41	25%

Partint dels resultats obtinguts i exposats a l'annex A.P i A.E, podem determinar que l'empresa XXXX ha millorat l'estat de la seva seguretat en el seu SGSI amb l'aplicació de les bones pràctiques i guies definides per la norma ISO/IEC 27002:2013 situant-se així a un grau de maduresa del SGSI superior al 80%.



En l'annex B.P es recull el raonament i determinació de compliment dels objectius marcats per l'any d0'aquesta iteració del SGSI marcats per l'empresa en funció dels controls i projectes que s'han dut a terme, que han afectat així al compliment dels controls establerts per la norma i a assolir el grau de compliment anteriorment exposat.

8.2 Resum executiu

En l'annex Resum executiu es troba un document introductori, sintetitzat o resumit amb la descripció de la tasca realitzada en el projecte d'avaluació i millora de l'estat de la seguretat del SGSI de la nostra organització. Aquest resum consisteix en una petita introducció a mode de resum simplificat per a la percepció inicial de les tasques, objectius i propòsits del nostre Sistema Gestor de la Seguretat de la Informació.

10. Conclusions

Amb la realització d'aquest projecte s'ha aconseguit satisfactòriament assolir l'objectiu plantejat inicialment, consistent en determinar i analitzar segons la norma ISO/IEC 27001 i el codi de bones pràctiques associat el Sistema Gestor de la Seguretat de la Informació, en una empresa situada en una dimensió o marc d'0actuació reals; podent desenvolupar i analitzar l'estat de la seguretat que dona continuïtat al negoci.

D'aquesta manera s'ha pogut analitzar, plantejar i determinar totes les fases plantejades per la norma aplicades ne el nostre cas d'estudi (l'empresa XXXX).

S'ha dut a terme l'anàlisi de riscos i amenaces de l'empresa XXXX així com la proposta i planificació de projectes per a incrementar el nivell de compliment i seguretat de la norma ISO per a la nostra empresa.

Com a ampliacions possibles per aquest projecte contemplaria la possibilitat de desenvolupar amb més detall (en funció de les àrees i actius concrets) de les tecnologies, contractes i aspectes més detallistes dels projectes de millora que no s'han arribat a tractar, l'anàlisi del mateix cas d'estudi en una segona (o inclús tercera i quarta) iteració del procés de millora i implantació del SGSI.

11. Glossari

Informació: En l'àmbit informàtic, contingut d'una o més dades amb significat, en un suport determinat i que aporta contingut i redueix la incertesa de les decisions que prenem.

Seguretat de la informació: Conjunt de mesures de prevenció i reacció de les organitzacions i dels sistemes tecnològics que permeten protegir i resguardar la informació per a mantenir-ne la confidencialitat, disponibilitat i integritat.

Actiu: son els bens, serveis i infraestructures amb capacitats funcionals i operatives necessaris per al desenvolupament de l'activitat soci-econòmica d'una empresa; podent variar segons la naturalesa de l'activitat desenvolupada.

Risc: Contingència a la qual esta exposat algú o alguna cosa.

Amenaça: Fet pel qual es manifesta un perill o una cosa a témer.

Vulnerabilitat: debilitat en els procediments de seguretat, disseny, implementació o control intern que podria ser explotada i que resulta en una bretxa de seguretat o una violació de la política de seguretat de sistemes.

Incident: Fet que es produeix en el transcurs d'algun assumpte o procés repercutint sobre aquest alterant-lo o interrompent-lo.

Disponibilitat: Característica, qualitat o condició de la informació d'estar a disposició de qui te que accedir-hi en el moment que sigui necessari.

Confidencialitat: Propietat que impedeix la divulgació de la informació a individus, entitats o processos no autoritzats; assegurant l'accés a la informació únicament per aquells que hi estan autoritzats.

Integritat: Propietat que permet mantenir les dades lliures de modificacions no autoritzades.

Traçabilitat: La propietat del resultat d'una mesura o valor d'un estàndard on aquest pugui relacionar amb referències específiques a través d'una cadena continua de comparacions totes les incerteses específiques. En resum, la capacitat de coneixença de l'origen, la composició, la història dels processos aplicats i la distribució i localització d'una informació.

Autenticitat: Propietat que permet identificar l'origen de la informació.

Cicle Deming (PDCA): estratègia de millora continua de qualitat en quatre fases: Planificar, Fer, Verificar/Controlar i Actuar (PDCA, segons les inicials en anglès). Els resultats d'aquest cicle permeten a les empreses la millora integral millorant contínuament la qualitat i reduint riscos i costos.

Polítiques de seguretat de la informació: Documentació d'alt nivell que recull i manifesta el compromís de la gerència amb la seguretat de la informació, contenint el pint de vista d'una entitat en aquest àmbit.

12. Bibliografia

Ministerio de administraciones públicas, "MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información" – Método. Versión 2, España, 2006. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VxDx2jCLSUk

INCIBE,"Sistemas de Gestión de la Seguridad de la Información en una Organización"- vídeo https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html

El Portal de ISO 27001 En Español, "Guia de Controles IDO 27002:2013". http://www.iso27000.es/

El Portal de ISO 27001 En Español, "Nuevo Glossario ISO 27000:2014". http://www.iso27000.es/

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES, octubre 2013, ISO2700.es. http://www.iso27000.es/download/ControlesISO27002-2013.pdf

ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls (segona edició). http://www.iso27001security.com/html/27002.html

The ISO 27001 and ISO 27002, Information Security Community Portal. http://www.17799.com/

Jan Devos,Hendrik van Landeghem,Dirk Deschoolmeester, "Information Systems for small and medium-sized enterpises: State of Art of IS Research in SMEs. Springer-Verlag Berlin Heidelberg 2014. Information Systems for Small and Medium-sized Enterprises...

13. Annexos

Annex A.E: Document extern al document en format Excel que conté l'anàlisi dels controls que estableix la norma ISO/IEC estudiada per al seu compliment en les diferents fases del projecte.

Annex B.E: Document extern al document en format Excel que conté l'anàlisi de riscos i taules generades per a la proposta de projectes de millora del sistema.

Annex A.P: Document extern al document en format PDF que conté l'anàlisi del compliment de la norma ISO estudiada.

Annex B.P: Document extern al document en format PDF que conté l'anàlisi del compliment dels objectius de negoci al final del procés.

Resum executiu: Document extern al document en format PDF amb el resum executiu del SGSI.