Implementació d'un Pla director de seguretat.

Nom Estudiant: Salvador Gavarró Llauradó

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

Nom Consultor: Arsenio Tortajada Gallejo

Centre: Universitat Oberta de Catalunya

Data Lliurament: 05/06/2019

FITXA DEL TREBALL FINAL

Títol del treball:	*Implementació d'un pla director de seguretat en una empresa del sector turístic.*
Nom de l'autor:	*Salvador Gavarró Llauradó*
Nom del consultor:	*Arsenio Tortajada Gallego.*
Data de lliurament (mm/aaaa):	*06/2019*
Àrea del Treball Final:	*Sistemes de Gestió de la seguretat de la informació*
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

El següent projecte correspon al Treball Final del Màster - TFM del "Màster interuniversitari de Seguretat de les tecnologies de la informació i de les comunicacions- MISTIC" de la universitat Oberta de Catalunya, Universitat Rovira i Virgili i la Universitat Autònoma de Barcelona, en el qual es defineix la planificació i disseny d'un sistema de gestió de seguretat SGSI així com la implementació d'alguns dels elements, basat en la norma ISO / IEC 27001: 2005 i el seu annex la ISO 27002, aquest projecte està dirigit a una empresa del sector turístic català i està emmarcat d'acord a l'abast i la declaració d'aplicabilitat definida.

El SGSI segueix el procés/cicle de Deming (Planejar-Fer-Verificar-Actuar) i donar una aplicabilitat del que és la implantació d'un SGSI en pro de la protecció de la informació.

De la mateixa manera, en la proposta d'implementació de controls s'han de tenir en compte la normativitat i legislació actual existent a España, en concret la RGPD i LOPD.

Abstract (in English, 250 words or less):

This project corresponds to the Final Master's Degree - TFM of the "Màster interuniversitari de Seguretat de les tecnologies de l'informació i de comunicacions- MISTIC" of the Open University of Catalonia, Universitat Rovira i Virgili and the Universitat Autònoma de Barcelona, in the What is defined is the planning and design of a security management system, with the implementation of some of the elements, based on ISO / IEC 27001: 2005

and the annexation of ISO 27002, which is directed to a company in the catalan tourism sector.

Paraules clau (entre 4 i 8):

SGSI, TFM, ciberseguretat, ISO27001, ISO 27002

1 Index

1 Introducció.

1.1 Context i justificació del treball.

L'objecte d'anàlisis d'aquest treball és crear un pla director de seguretat per implantar-lo en un grup d'empreses situades a la Costa Daurada dedicades al turisme i als events esportius, a efectes d'aquest treball l'anomenarem SCP.

La principal raó que ha motivat la tria d'aquesta temàtica ha estat la gran rellevància que té el correcte funcionament del sistemes informàtics i de telecomunicacions en una regió que troba el motor de la seva economia en el turisme esportiu, de sol i platja.

Tanmateix, la meva implicació directa com a CIO amb SCP, n'ha estat un factor determinant en la presa d'aquesta decisió.

La seguretat de la informació és una qüestió que afecta tota la companyia, ja que tota l'organització treballa amb informació i, per tant, requereix una gestió coordinada i transversal, la qual cosa comporta planificació i gestió, i no pot ser improvisat, sinó que ha de ser considerat com un procés més de la companyia que interactua amb la resta dels processos del negoci.

El sector turístic i d'hoteleria és una de les principals bases i motors de l'economia catalana i espanyola. Catalunya i Espanya són destins turístics que disposen d'un patrimoni cultural molt variat que atrau a milions de turistes cada any, tant internacionals com nacionals.

El sector turístic i d'hoteleria es composa per tres grans àmbits d'activitat: la restauració, que compren les activitats associades a la provisió de menjar i beguda; l'allotjament, que engloba les activitats de pernoctació que es desenvolupen en els hotels, càmpings, resorts, cases rurals i albergs, entre d'altres; i, per últim, la planificació, gestió i comercialització turística, que engloba les activitats destinades a la gestió de serveis turístics a través de tercers, agències de viatges majoristes o minoristes.

El grup d'empreses subjecte a l'estudi són dos complexes turístics i un complex esportiu que ofereix la més àmplia gama de serveis, així com les millors i més modernes instal·lacions. Concretament, presenta serveis d'hoteleria (allotjament, menjar i beguda), d'oci, d'esport, de compres i d'altres.

Estan ubicats a Cambrils i Salou (Costa Daurada) i, en els últims anys, han estat premiats amb nombrosos premis de reconeixement a nivell Europeu (veure **Annex 1**).

SCP disposa de més de 1000 bungalows, més de 1000 parcel·les per caravanes o tendes, 20 Camps de futbol, camps de rugbi, futbol platja, mini estadi ,etc..

En màxim moment d'ocupació poden haver 10.000 persones allotjades en temporada alta.

Aquest grup d'empreses compta amb una plantilla de 200 persones fixes que treballen els 365 dies de l'any, i amb una plantilla estacional de fins a 800 que presta serveis només als mesos d'obertura del Resort, és a dir, durant la temporada turística tradicional.

SCP no disposa d'un Sistema de Gestió de la Seguretat de la Informació de manera que aquest Treball pot ser la base de un futur procés d'implantació i certificació si així es decidís.

La informació que disposa SCP a trets generals prové d'aquestes fonts:

- Treballadors:
- Proveïdors:
- Clients:
- Pròpia:

1.1 Abast del SGSI.

La gestió de sistemes de seguretat d'informació en totes les activitats relacionades amb la creació, disseny, anàlisi, modificacions i proves de tota la documentació classificada com a privada i tota la infraestructura IT dels grup SCP , el sistema de Gestió de Seguretat de la Informació comprèn els sistemes d'informació que donen suport als processos de de gestió, allotjament, punts de venta i complex esportiu, d'acord amb la declaració d'aplicabilitat versió 1.0.

Aquesta normativa s'aplica a tots els ordinadors i sistemes en xarxa, administrats per la companyia o de la seva propietat.

De la mateixa manera, s'aplicarà a totes les plataformes (sistemes operatius), ordinadors de qualsevol grandària (ordinadors personals d'arquitectura client-servidor) i tots els sistemes d'aplicació (ja siguin aquells desenvolupats interiorment o comprats a tercers).

En el cas que certa informació quedi fora de l'abast es transferirà la responsabilitat mitjançant contractes als tercers que gestionin aquesta informació.

Aquest abast està delimitat per la declaració d'aplicabilitat i la implementació de controls es limita pel possible pressupost aprovat.

1.2 Objectius del treball.

- Garantir el funcionament de SCP oferint un servei d'alta disponibilitat, especialment en els serveis més crítics.
- Adaptar-se a les mesures de seguretat estrictament legals com a mínims que s'hauran reforçar amb d'altres mesures voluntàries.
- Millorar la confidencialitat, la integritat i la disponibilitat de la informació adoptant mesures de control tant organitzatives com tècniques.
- Identificar, qualificar i fer un tractament adequat dels riscos que puguin impactar negativament la informació, els processos de l'organització.

- Implantar tècniques que permetin detectar usos indeguts de la informació.
- Minimitzar les possibilitats de fugida o mal ús de la informació:
- Control de les cessions de dades a tercers.
- Control d'extracció de dades en suports informàtics o telemàticament.
- Reforç de les mesures de seguretat dels treballadors i clients.
- Custòdia adequada de documents i suports.
- Adequada tractament de les dades en suport paper en finalitzar la seva utilitat.
- Millorar el tractament de les incidències.
- Integrar les mesures anteriors en els procediments operatius diaris sense perjudicar l'eficàcia ni l'eficiència.
- Alineament i compromís de la direcció amb la seguretat de la informació.
- Oferir valor i confiança als clients a través de la millora en els sistemes i la seva adequada gestió..
- Fomentar la presa de consciència davant els riscos associats a la informació.

- Complir la normativa legal de seguretat, en particular de la RGPD i la Llei Orgànica de protecció de dades de caràcter personal (LOPD en endavant) i el seu Reglament.

1.3 Planificació del treball

1.3.1 Fase 1: Situació actual: Contextualització, objectius i anàlisis diferencial .

Introducció al Projecte. Enfoc i selecció de l'empresa que serà objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisis diferencial de l'empresa amb respecte a la ISO/IEC 27001+ISO/IEC 27002

1.3.2 Fase 2: Sistema de Gestió Documental.

Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI

1.3.3 Fase 3: Anàlisis de riscos.

Elaboració d'una metodologia d'anàlisis de riscos: Identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.

1.3.4 Fase 4: Proposta de Projectes.

Avaluació de projectes que ha de portar a terme la Organització per alinear-se amb els objectius plantejats al Pla Director. Quantificació econòmica i temporal d'aquests.

1.3.5 Fase 5: Auditoria de Compliment de la ISO/IEC 27002:2013.

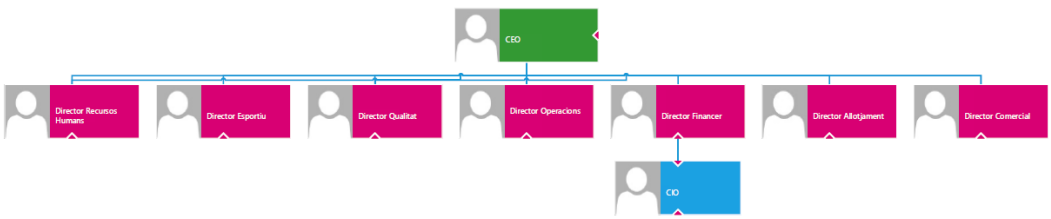
Avaluació de controls, maduresa i nivell de compliment.

1.3.6 Fase 6: Presentació de Resultats i entrega de Informes.

Consolidació dels resultats obtinguts durant el procés d'anàlisis. Realització dels informes i presentació executiva a Direcció. Entrega del projecte final.

2 Anàlisi de la situació Actual.

2.1 Estructura organitzativa.



2.2 Infraestructura IT.

L'àrea d'Infraestructura de TI té com a responsabilitat la gestió de tota la infraestructura tecnològica dels dos ressort i del complex esportiu, està composta de les següents plataformes e instal·lacions:

2.2.1 Infraestructures.

2.2.1.1 CPDs

En cada Ressort existeix una CPD, en aquest TFM la CPD del ressort CP l'anomenarem CPD1 i la CPD del ressort SG l'anomenarem CPD2.

Les dos CPDs estan unides entre elles per:

- 96 fibres monomode
    - 48 fibres monomode per una camí físic.
    - 48 fibres monomode per un altre camí físic.

La CPD2 està unida amb el complex esportiu per dos radioenllaços.

- 1 radio enllaç de 1Gb/s
- 1 radio enllaç de 200Mb/s de backup.

Tota la resta de edificis i locals estan units per fibra amb la CPD1 i CPD2, en la majoria de casos comparteixen part del camí físic.

2.2.1.2 Sistemes

2.2.1.2.1 Servidors:

- Windows server 2012
- Windows Server 2019
- Debian
- Gentoo

2.2.1.2.2 Bases de dades:

- SQL Server
- HF SQL
- Mysql

2.2.1.3 Cloud

- Reserves Online
- Office 365
- Kmkey

2.2.1.4 Xarxes

2.2.1.4.1 Routers:

- L'organització disposa de dos routers amb dos sortides a internet, els dos routers estan ubicats a la CPD1.

2.2.1.4.2 Tallafocs.

- L'organització disposa de dos tallafocs Fortigate en clúster un en cada CPD.

2.2.1.4.3 Switching

- La xarxa de switching està composta per 248 switchs.
    - CORE de 4 switchs en stack, 2 d'ells ubicats en cada CPD.
    - La resta de switchs dones servei a totes les altres infraestructures físiques.

2.2.1.5 TPVS

- L'Organització disposa de 50 TPVs, la gran majoria es Windows 10, encara que hi ha una petita part amb XP, està previst canviar-los aquest any 2019.

2.2.1.6 Estacions de treball.

La majoria de les estacions de treball són ordinadors de sobretaula tenen Windows 10 excepte una petita minoria que tenen Windows 7, està previst migrar totes les estacions de treball a Windows 10 aquest any 2019.

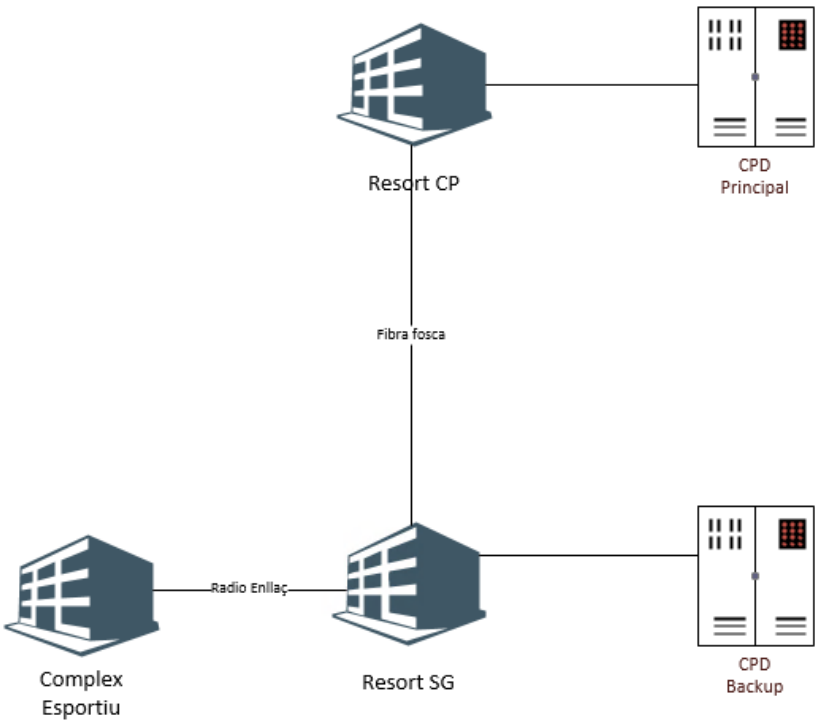
Excepcionalment l'organització disposa d'ordinadors portàtils per als empleats, tots ells tenen Windows 10.

2.2.1.7 Dispositius Mòbils.

Totes els empleats que ho necessiten disposen d'un terminal android.

Tots els directors disposen de terminals Iphone, alguns dels caps de sector excepcionalment també disposen de terminals Iphone.

2.2.2 Mapa general dels tres negocis.



Estan els dos ressorts units per fibra monomode, 2 cables de 48 fibres cada un, el camí dels dos cables és diferent en un 80% del trajecte.

El Complex esportiu està connectat per un radio enllaç de 1Gb de velocitat amb el ressort SG.

2.2.3 Mapa general del Resort CP.

2.2.4 Mapa general del Resort SG.

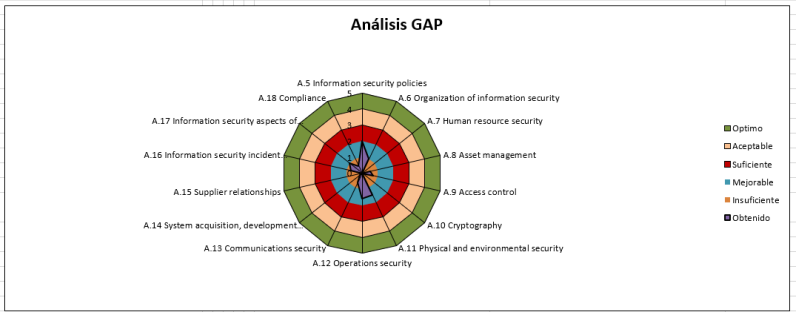
2.2.5 Mapa general del Complex Esportiu.

2.3 Anàlisi diferencial.

En aquesta apartat es realitzarà un anàlisi diferencial(GAP) contrastant els controls implantats versus els necessaris.

Amb el present anàlisi diferencial es pretén conèixer la distància entre la situació actual i el SGSI projectat, tant del que s'especifica en la ISO / IEC 27001: 2005 com a la ISO / IEC 27002: 2005.

	Valor
A.5 Information security policies	2
A.6 Organization of information security	1
A.7 Human resource security	0
A.8 Asset management	0,5
A.9 Access control	0,73
A.10 Cryptography	0
A.11 Physical and environmental security	1,5
A.12 Operations security	1,6
A.13 Communications security	0,65
A.14 System acquisition, development and maintenance	0,2
A.15 Supplier relationships	0
A.16 Information security incident management	0,7
A.17 Information security aspects of business continuity management	1
A.18 Compliance	0,5



Es constata que l'estat inicial de la seguretat de la informació és molt més baix del que es pensava inicialment:

- Tan sols es frega el suficient en 1 aspecte.
- En la majoria dels altres aspectes (9) és insuficient o inexistent.
- En els restants(4) és millorable però insuficient.

Aquest anàlisi complert es pot trobar en l'ANNEX 1 en la seva versió actual.

3 Sistema de gestió documental

3.1 Introducció

El pla director de seguretat o SGSI ha de tenir una sèrie de documents, els quals venen establerts en la pròpia norma ISO / IEC 27001. A continuació es descriuen aquests documents, els quals poden ser observats en els annexos corresponents.

3.2 Esquema documental

ISO / IEC 27001 defineix quins són els documents necessaris per poder certificar el sistema, però per al desenvolupament del treball van ser necessaris els següents documents:

3.2.1 Política de seguretat

Normativa interna que ha de conèixer i complir tot el personal afectat per l'abast del Sistema de Gestió de Seguretat de la Informació.

El contingut de la Política ha de cobrir aspectes relatius a l'accés de la informació, ús de recursos de l'Organització, comportament en cas d'incidents de seguretat, etc.

Aquesta política es troba en procés de realització i revisió perquè pugui entrar en fase d'actualització i posteriorment a la seva aprovació per part de la gerència .

Aquesta política encara es troba en fase d'actualització i aprovació per part de l'alta direcció, i en alguns aspectes encara és genèrica, per la qual cosa es recomana a l'empresa un ajust abans de la seva aprovació per poder ser presentada als seus empleats.

Aquesta política de seguretat es defineix en l'ANNEX 2 en la seva versió actual.

3.2.2 Procediment d'Auditories Internes

Document que ha d'incloure una planificació de les auditories s'establiran als auditors interns i es definirà el model d'informe d'auditoria.

En aquest cas com que l'Organització ja té definit un procediment les auditories internes referents el procediment s'alinearà amb sistema actual ja definit d'auditories internes.

En l'ANNEX 3 hi ha el pla d'auditories internes en la seva versió actual.

3.2.3 Gestió d'indicadors.

Cal definir indicadors per mesurar l'eficàcia dels controls de seguretat implantats. Igualment és important definir la sistemàtica per mesurar-los.

Aquests indicadors estaran alineats a la política de seguretat de l'empresa.

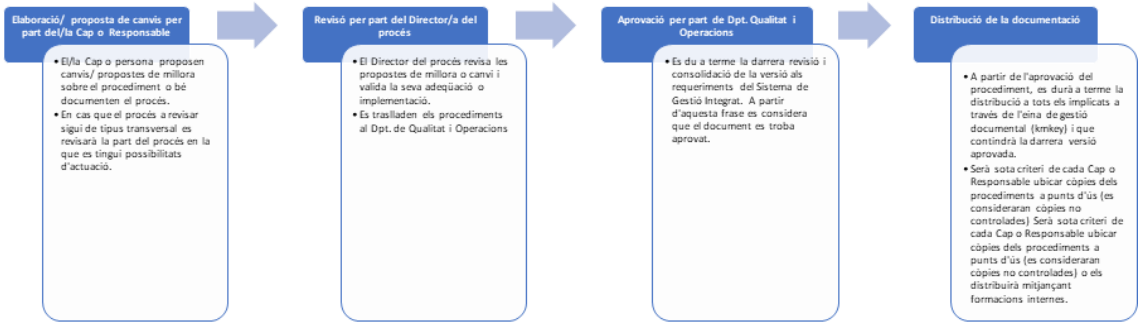
La norma ISO 27001 ens dona els punts de control necessaris i la norma 27004 ens indica com i els tipus de mesures a utilitzar.

En l'ANNEX 4 hi ha definits els indicadors en la seva versió actual.

3.2.4 Procediment de Revisió per Direcció.

La Direcció de l'empresa ha de revisar anualment les qüestions més importants que han succeït en relació al Sistema de Gestió de Seguretat de la Informació.

Per a aquesta revisió, la ISO / IEC 27001 defineix tant els punts d'entrada, com els punts de sortida que s'han d'obtenir d'aquestes revisions.



Aquest procediment es defineix en l' ANNEX 5.

3.2.5 Gestió de Rols i Responsabilitats.

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, ha d'estar compost almenys per una persona de Direcció, així garantim el suport i l'alineació amb l'alta direcció, en aquest cas la persona designada es el director financer que també és el responsable final del departament de informàtica, d'aquesta manera les decisions que es prenguin estaran recolzades per un directiu.

Aquestes responsabilitats i rols es detallen en l' ANNEX 6 en la seva versió actual..

3.2.6 Metodologia d'Anàlisi de Riscos.

En aquesta secció, s'estableix un procés sistemàtic que se seguirà per calcular el risc, la qual cosa ha d'incloure bàsicament la identificació i valoració dels actius, amenaces i vulnerabilitats.

Aquesta metodologia es detalla a l' ANNEX 7 en la seva versió actual.

3.2.7 Declaració d'Aplicabilitat.

Document que inclou tots els controls de seguretat establerts en l'Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada.

És un document que reflecteix el perfil de seguretat d'una empresa, aquí es declaren els controls que són rellevants per al SGSI de l'àrea d'operacions i aplicables a aquest.

La norma ISO27002 ens dona informació sobre la seva impmabtació.

La Declaració d'aplicabilitat proposta es detalla a l' ANNEX 8 i l'ANNEX 8.1.

4 Estat del risc: Identificació i valoració.

En aquesta secció es calcular el risc, la qual cosa ha d'incloure bàsicament la identificació i valoració dels actius, amenaces i vulnerabilitats i càlcul del seu risc.

En una segona part és fa el tractament del risc.

Aquesta metodologia es detalla a l' ANNEX 9.1 i en la fulla de càlcul en la seva versió actual.

5 Proposta de projectes.

La competència del Comitè de Seguretat a l'elaboració d'un pla de tractament de les

Amenaces detectades al pla de riscos del apartat numero 4 d'aquest document.

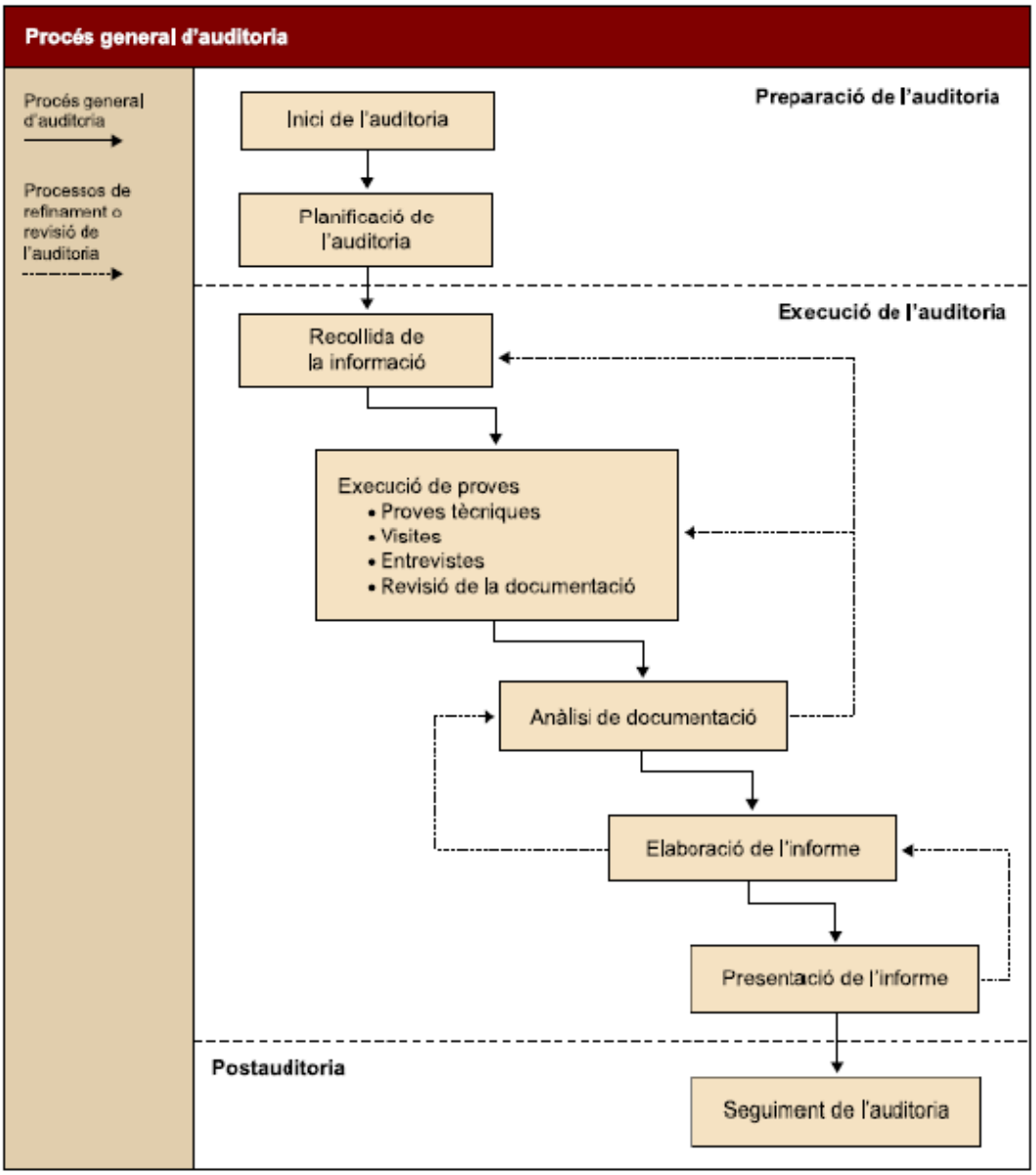
Aquest pla de tractament ha d'estar alienat amb els objectius del Pla Director descrits en l'apartat 1.2.

Analitzen el pla de riscos podem decidir sobre els controls a aplicar per reduir els riscos detectats.

Aquesta pla de projectes es detalla a l' ANNEX 10 en la seva versió actual.

6 Auditoria de compliment de la ISO27001/2013

Aquesta apartat es definiex una revisió sistemàtica del compliment dels criteris d'auditoria definits en les ISO2001, ISO27002 i ISO 27004.



Aquesta informe d'auditoria es detalla a l' ANNEX 11 en la seva versió actual.

7 Glossari.

- **SGSI**

Sistema de gestió de la seguretat de la informació.

- **CISO**

Director de la Seguretat de la Informació

- **Anàlisis de riscos**

Estudi de les causes de les possibles amenaces i probables esdeveniments no desitjats iels danys i conseqüències que aquestes puguin produir.

- **Dades de caràcter personal**

Informació referent a persones físiques identificades o identificables

- **Gestió d'incidents**

Pla d'acció per atendre les incidències que es donin. A més de resoldre-ho d'incorporar mesures d'acompliment que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

- **Política de seguretat**

Conjunt de normes que donen instruccions de com una organització gestiona i protegeix la informació i els actius.

- **Actiu.**

Elements que són necessaris per al normal funcionament de l'organització

- **Amenaça**

Perills que desencadenen en un incident a l'empresa, realitzant un dany material o pèrdues de servei dels seus actius.

- **Vulnerabilitat.**

Possibilitat que es materialitzi una amenaça sobre un actiu.

- **Impacte.**

Dany que es produeix quan una amenaça aprofita una vulnerabilitat per afectar el funcionament d'un actiu.

8 Bibliografia.

- **Material Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i les Comunicacions**

Assignatura SGSI.

Mòdul 1 - Introducció a la seguretat de la informació

Mòdul 2 - Anàlisi de riscos

Mòdul 3 - Implantació d'un sistema de gestió de la seguretat de la informació (SGSI)

Mòdul 4 - Desenvolupament d'alguns objectius de control de l'SGSI

Mòdul 5 - Plans de continuïtat de negoci

Assignatura Auditoria Tècnica:

Mòdul 2 - Auditoria de certificació ISO 27001

Mòdul 3 - Auditoria tècnica de seguretat de sistemes d'informació i comunicacions

- **ISO/IEC27000**

http://www.iso27000.es/iso27002.html

9 Annexos.

- Annex 1 – Anàlisi GAP-Diferencial
- Annex 2 – Política de Seguretat
- Annex 3 - Procediment d'Auditories Internes
- Annex 4 - Gestió d'Indicadors
- Annex 5 - Procediment de Revisió per Direcció
- Annex 6 - Gestió de Rols i Responsabilitats
- Annex 7 - Metodologia de Anàlisis de Riscos
- Annex 8.1 - Declaració de Aplicabilitat
- Annex 9.1 - Anàlisi de Riscos
- Annex 10 - Proposta de projectes
- Annex 11 – Auditoria
- Annex 12 – Anàlisi GAP Actual

9.1 Annex 1 – Analisi GAP-Diferencial

1. Introducció

Amb el present anàlisi diferencial es pretén conèixer la distància entre la situació actual i el SGSI projectat, tant del que s'especifica en la ISO / IEC 27001: 2005 com a la ISO / IEC 27002: 2005.

2. Notació.

Per a l'avaluació del grau de compliment es seguirà una notació de 0 a 5 de forma similar al Model de Maduresa, les equivalències són les següents:

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

3. Analisi

Control	ID	Nivell	Comentaris
5-Polítiques de seguretat.	2	Repetible	
5.1-Directrius de gestió de seguretat de la informació	2	Repetible	
5.1.1-Politiques de seguretat de la informació	2	Repetible	
5.2-Revisió de les polítiques de seguretat de la informació	2	Repetible	
6-Organització de la Seguretat de la Informació.	1,5	incial	
6.1-Organització Interna	1	Incial	
6.1.1 Rols i responsabilitat en la seguretat de la informació	1	Inicial	

6.1.2- segregació de tasques	0	No definit	
6.1.3-Contacte amb les autoritats	0	No definit	
6.1.4-Contacte amb grups d'interès especial	2	Repetible	
6.1.5- Seguretat de la informació en la gestió de projectes.	1	Inicial	
6.2- Dispositius mòbils i teletreball	2	Repetible	
6.2.1-Política de dispositius mòbils	2	Repetible	
6.2.2-Teletreball	2	Repetible	
7-Seguretat dels Recursos Humans.	0	No existent	
7.1- Abans de treballar	0	No existent	
7.1.1-Investigació Antecedents	0	No existent	
7.1.2-Termes i condicions de treball	0	No existent	
7.2- Durant el treball	0,3	No existent	
7.2.1-Responsabilitats de gestió	0	No existent	
7.2.2-Concienciació, educació i capacitació en seguretat de la informació.	1	Inicial	
7.2.3-Procés disciplinari.	0	No existent	
7.3 – Finalització o canvi de treball	0	No existent	
7.3.1-Responsabilitats davant la	0	No existent	

finalització o canvi.		
8-Gestió dels Actius.	0,5	No existent
8.1-Responsabilitat Actius	0	No existent
8.1.1-Inventari Actius	0	No existent
8.1.2-Propietat dels actius.	0	No existent
8.1.3-ús acceptable dels actius.	0	No existent
81.4-Devolució dels actius.	0	No existent
8.2- Classificació de la informació	0,6	No existent
8.2.1-Classificació de la informació	2	Repetible
8.2.2-Etiquetat de la informació.	0	No existent
8.2.3-Manipulat de la informació.	0	No existent
8.3- Manipulació dels suports	1	Inicial
8.3.1-Gestió de suports extraïbles.	1	Inicial
8.3.2-Eliminació de suports	1	Inicial
8.3.3-Suports físics en transit.	1	Inicial
9-Control d'Accessos.	0,73	No Existent
9.1 Requisits de negoci per el control d'accés.	1	Inicial
9.1.1-Politica control accés	1	Inicial
9.1.2-Accés a les xarxes i serveis de xarxa.	2	Repetible
9.2 Gestió d'accés d'usuari	0	No Existent

9.2.1-Registre i baixa d'usuaris	0	No Existent	
9.2.2-Provisió d'accés d'usuari.	0	No Existent	
9.2.3-Gestió de privilegis d'accés.	0	No Existent	
9.2.4-Gestió de la informació secreta d'autenticació dels usuaris.	0	No Existent	
9.2.5-Revisiaó dels drets d'accés d'usuari.	0	No Existent	
9.2.6-Retirada o reasignació dels drets d'accés.	0	No Existent	
9.3- Responsabilitats de l'usuari	0	No Existent	
9.3.1-Ús de la informació secreta d'autenticació.	0	No Existent	
9.4- Control d'acces a sistemes i aplicacions	1,2	Inicial	
9.4.1-Restricció de l'accés a la informació	1	inicial	
9.4.2-Procediments segurs d'inici de sessió.	1	inicial	
9.4.3-Sistema de gestió de contrasenyes.	2	repetible	
9.4.4-Ús d'utilitats amb privilegis de sistema.	1	inicial	
9.4.5-Control d'accés al codi font del programari.	1	inicial	
10-Criptografia	0	No Existent	
10.1-Controls criptogràfics	0	No Existent	

10.1.1-Política d'ús de controls criptogràfics.	0	No Existent	
10.1.2-Gestió de claus.	0	No Existent	
11-Seguretat física i ambiental.	1,5	Inicial	
11.1- Areas segures	1	Inicial	
11.1.1-Perímetre de seguretat Fisica	2	repetible	
11.1.2-Controls físics d'entrada	2	repetible	
11.1.3-Seguretat d'oficines, despatxos i recursos.	1	Inicial	El grups que van a les sales de conferencies tenen accés a les oficines.
11.1.4-Protecció contra perills externs i ambientals.	0	No definit	
11.1.5-El treball en hores segures.	0	No definit	
11.1.6-Àrees de carrega i descarrega.	2	Repetible	
11.2- Seguretat dels equips	2	Repetible	
11.2.1-Emplaçament i protecció d'equips.	2	Repetible	
11.2.2-Instal·lacions de subministrament.	2	Repetible	
11.2.3-Seguretat del cablejat.	2	Repetible	
11.2.4-Manteniment dels equips.	2	Repetible	
11.2.5-Retirada de materials propietat de l'empresa.	2	Repetible	

11.2.6-Seguretat dels equips fora de les instal·lacions.	2	Repetible	
11.2.7- Reutilització o eliminació segura dels equips.	2	Repetible	
11.2.8-Equip d'usuari desatés.	2	Repetible	
11.2.9-Política de lloc de treball buidat i pantalla neta.	2	repetible	
12-Seguretat de les Operacions.	1,6	Inicial	
12.1- Procediments i responsabilitats operacionals	1	Inicial	
12.1.1- Documentació de procediments de les operacions.	1	Inicial	
12.1.2-Gestió de canvis.	0	No Existent	
12.1.3-Gestió de capacitats	2	Repetible	
12.1.4-Separació dels recursos de desarrollo, prova	2	repetible	
12.2- Protecció contra malware	2	repetible	Si es documenta pasaria a nivell 3
12.2.1-Controls contra el codi maliciós.	2	repetible	Si es documenta pasaria a nivell 3
12.3- Copies de seguretat	4	Gestionat	
12.3.1-Copies de seguretat de la informació.	4	gestionat	
12.4- Registres i supervisions	1,75	Inicial	
12.4.1-Registre d'events.	2	Repetible	

12.4.2-protecció de la informació de registre.	2	Repetible
12.4.3-Registre d'administració i operacions.	1	Inicial
12.4.4_sincronització del rellotge.	2	Repetible
12.5- Control de software explotació	0	No existent
12.5.1-Instal·lació del programari en explotació.	0	No existent
12.6- Gestió de vulnerabilitat tècnica	2	Repetible
12.6.1-gestió de la vulnerabilitat tècniques	1	Inicial
12.6.2-Restricció en la instal·lació de software.	3	Definit
12.7- Consideracions sobre auditoria de sistemes de informació.	1	Inicial
12.7.1-Controls d' auditoria de sistemes de informació	1	Inicial
13-Seguretat de les Comunicacions.	0,65	No existent
13.1- gestió de la seguretat de xarxa.	1,3	Incial
13.1.1-Controls de xarxa.	1	Inicial
13.1.2-Seguretat dels serveis de xarxa.	1	Incial
13.1.3-Segregació en xarxes.	2	Repetible
13.2- Intercanvi de informació	0	No existent

13.2.1-Polítiques i procediments d'intercanvi d'informació.	0	No existent	
13.2.2-Acords d'intercanvi d'informació	0	No existent	
13.2.3-Missatgeria electrònica.	1	Inicial	
13.2.4_acords de confidencialitat i no revelació.	1	Incial	
14-Adquisició de sistemes, desenvolupament i manteniment: requisits de seguretat dels sistemes d'informació.	0,2	No Existent	
14.1Requisite de la seguretat de la informació	0,6	No Existent	
14.1.1-Requisits de seguretat en els sistemes d'informació.	1	Inicial	
14.1.2- Assegurar els serveis d'aplicacions de xarxes publiques.	1	Inicial	
14.1.3- protecció de les transaccions de serveis d'aplicacions.	0	No Existent	
14.2-Seguretat en el desenvolupament i en els processos de suport.	0,2	No Existent	
14.2.1-Política de desenvolupament segur.	0	No Existent	
14.2.2_Procedimen t de control de canvis en sistemes.	0	No Existent	

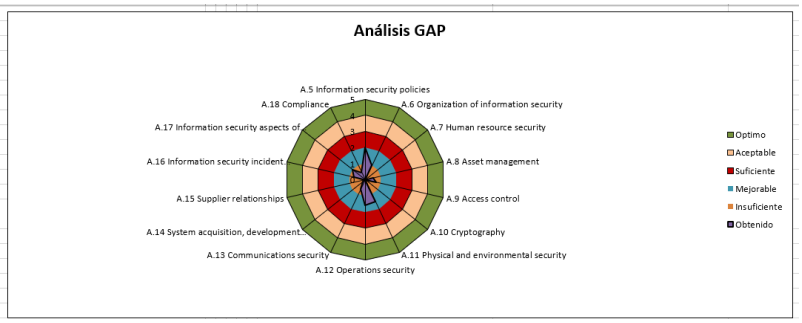
		14.2.3-revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu.	0	No Existent
		14.2.4_Restriccions als canvis en el paquests e software.	0	No Existent
		14.2.5_Principis d'enginyeria de sistemes segurs.	0	No Existent
		14.2.6-Entorn de desenvolupament segur.	1	Inicial
		14.2.7-Externalització del desenvolupament	1	Incial
		14.2.8-Proves funcionals de seguretat de sistemes	0	No existent
		14.2.9-Proves d'acceptació de sistemes.	0	No existent
	14.3- Dades de prova.		0	No existent
		14.3.1-Protecció de les dades de prova.	0	No existent
15-Relacions amb els Proveïdors..			0	No existent
	15.1-Seguretat amb les relacions dels proveïdors.		0	No existent
		15.1.1-Política de seguretat de la informació a les relacions amb els proveïdors.	0	No existent
		15.1.2-Requisits de seguretat de contractes amb tercers.	0	No existent

15.1.3-Cadena de subministre de tecnologia de la informació i les comunicacions.	0	No existent	
15.2- gestió de la provisió dels serveis de proveïdor.	0	No existent	
15.2.1-Control i revisió de la provisió de serveis del proveïdor.	0	No existent	
15.2.2_Gestió de canvis a la provisió del servei del proveïdor.	0	No existent	
16-Gestió d'Incidències que afecten a la Seguretat de la Informació.	0,7	No Existent	
16.1- Gestió de incidències de seguretat de la informació i millores.	0,7	No existent	
16.1.1-Responsabilitats i procediments.	2	Repetible	
16.1.2-Notificació dels events de seguretat de la informació.	2	repetible	
16.1.3-Notificació de punts debils de la seguretat.	0	No existent	
16.1.4-Evaluació i decicisó sobre els events de seguretat de la informació	0	No existent	
16.1.5-Resposta a incidents de seguretat de la informació.	0	No existent	
16.1.6-Aprenentatge dels	0	No existent	

		incidents de seguretat de la informació		
		16.1.7-Recopilació d'evidencies.	1	Inicial
17-Aspectes de Seguretat de la Informació per a la Gestió de la Continuïtat del Negoci.			1	Incial
	17.1- Continuïtat de seguretat de la informació		1	Incial
		17.1.1-Planificació de la continuïtat de la seguretat de la informació	2	Repetible
		17.1.2-Implementar la continuïtat de la seguretat de la informació.	2	Repetible
		17.1.3-Verificació, revisió i evaluació de la continuïtat de la seguratat de la informació.	2	repetible
	17.2-Redundancies		1	Inicial
		17.2.1-Disponibilitat de recursos de tractamentd e la informació.	1	Inicial
18-Conformitat.			0,5	No existent
	18.1- Compliment de requisits legals i contractuals		1	Inicial
		18.1.1-Identificació de la legislació aplicable i dels requisits contractuals.	1	Inicial
		18.1.2-Drets de propietat intel·lectual.	1	Inicial

		18.1.3-Protecció dels registres de l'organització.	1	Inicial	
		18.1.4-Protecció i privacitat de la informació de caràcter personal.	1	Inicial	
		18.1.5-Regulació dels controls criptogràfics.	1	Inicial	
	18.2- Revisions de la seguretat de la informació.		0	No existent	
		18.2.1-Revisió independent de la seguretat de la informació	0	No existent	
		18.2.2-Compliment de les polítiques i normes de seguretat	0	No existent	
		18.2.3-Comprovació del compliment tècnic.	0	No existent	

	Valor
A.5 Information security policies	2
A.6 Organization of information security	1
A.7 Human resource security	0
A.8 Asset management	0,5
A.9 Access control	0,73
A.10 Cryptography	0
A.11 Physical and environmental security	1,5
A.12 Operations security	1,6
A.13 Communications security	0,65
A.14 System acquisition, development and maintenance	0,2
A.15 Supplier relationships	0
A.16 Information security incident management	0,7
A.17 Information security aspects of business continuity management	1
A.18 Compliance	0,5



4. Conclusions

Es constata que l'estat inicial de la seguretat de la informació és molt més baix del que es pensava inicialment:

- Tan sols es frega el suficient en 1 aspecte.
- En la majoria dels altres aspectes (9) és insuficient o inexistent.

- En els restants(4) és millorable però insuficient.

9.2 Annex 2 – Política de Seguretat

9.2.1 Introducció.

En la societat actual, un dels principals béns que cal protegir, aquell que representa un valor més important per als negocis, és la informació, i per això hi ha aquesta necessitat de protegir-la, ja que el món està cada vegada més connectat, i els atacs a les infraestructures, les xarxes i els sistemes són cada vegada més sofisticats.

La seguretat de la informació és una qüestió que afecta tota la companyia, ja que tota l'organització treballa amb informació i, per tant, requereix una gestió coordinada i transversal, la qual cosa comporta planificació i gestió, i no pot ser improvisat, sinó que ha de ser considerat com un procés més de la companyia que interactua amb la resta dels processos del negoci.

Per garantir aquesta seguretat va sorgir el concepte el Sistema Gestor de la seguretat de la informació (SGSI) concepte central de la norma ISO27001, aquest sistema es basa en que la informació és un dels actius més importants de qualsevol companyia o organització, i com ha tal hi ha que protegir-lo.

Un SGSI és una eina allunyada de tecnicismes, que ofereix una visió global sobre l'estat dels sistemes d'informació.

9.2.2 Política de seguretat.

L' equip directiu és conscient de la importància que té per a la companyia la seguretat de la informació de cara a aconseguir un grau òptim de competitivitat al mercat actual. Per això s'ha desenvolupat la present Política de Seguretat i els corresponents procediments que garanteixin la confidencialitat, integritat i disponibilitat de la informació.
El responsable de seguretat amb la coordinació de la direcció ha pretès definir els processos més adequats perquè l'empresa emprengui un procés de millora dels seus Sistemes de Seguretat de la Informació amb el convenciment que redundarà en una major eficàcia dels seus processos de producció.
La intenció final de tot el sistema definit i desenvolupat és la d'oferir el millor servei als nostres clients, millorant els nostres processos i respectant escrupolosament els seus drets legalment establerts.
Per tot això, la direcció vol deixar constància expressa del seu coneixement i de la seva aprovació de les polítiques desenvolupades en aquest document, de manera que tot el personal les ha de conèixer i assumir com una part de les seves funcions laborals.

9.2.3 Normes de Seguretat.

9.2.3.1 Principis generals del SGSI

9.2.3.1.1 Paper de la informació i els sistemes de la informació

La informació i els sistemes informàtics són valors crucials i de vital importància per XXXXXXXXX,S.A (d'ara endavant la companyia).

Sense uns adequats sistemes, que protegeixin aquesta informació de forma eficaç, la seguretat, integritat i privacitat dels documents de la companyia podrien veure's compromesos.

Així mateix, la cura i augment de la reputació de qualsevol companyia està directament relacionat amb la manera en què la informació i els sistemes informàtics es gestionen.

El manteniment d'un nivell apropiat de seguretat és un dels aspectes més importants, tant per a la gestió d'informació com per la dels sistemes informàtics.

9.2.4 La seguretat com un treball en equip

Perquè la seguretat de la informació sigui efectiva, s'ha de dur a terme com una tasca en equip. Aquesta tasca requereix la participació i el suport de cadascun dels empleats de la companyia que tinguin accés a la informació i/o als sistemes informàtics.

D'acord amb tal necessitat de realitzar aquesta tasca com a part del treball d'equip, la present normativa aclareix les responsabilitats dels usuaris, així com els passos a seguir per protegir la informació de la companyia i els seus sistemes informàtics.

Aquest document descriu els procediments per prevenir i respondre davant algunes amenaces a la informació i els sistemes informàtics.

Entre ells s'inclouen: accessos no autoritzats, duplicació, apropiació, destrucció, pèrdua, mal ús, difusió d'informació, i rebuig a la seva utilització.

9.2.5 Persones involucrades

Tot treballador de la companyia, independentment de la seva posició (empleat, contractista, assessor, treballador temporal, etc.), ha de complir amb la normativa per a la seguretat d'informació descrita en aquest i successius documents relacionats amb la seguretat informàtica.

Aquells empleats que violin aquesta o altres normatives per a la seguretat del sistemes i la protecció de la informació estaran subjectes a les corresponents accions disciplinàries, arribant fins i tot a l'acomiadament.

9.2.6 Sistemes involucrats

Aquesta normativa s'aplica a tots els ordinadors i sistemes en xarxa, administrats per la companyia o de la seva propietat.

De la mateixa manera, s'aplicarà a totes les plataformes (sistemes operatius), ordinadors de qualsevol grandària (ordinadors personals d'arquitectura client-servidor) i tots els sistemes d'aplicació (ja siguin aquells desenvolupats interiorment o comprats a tercers).

Aquesta normativa comprèn únicament la informació que es maneja en els ordinadors i/o sistemes en xarxa. És a dir, encara que aquest document esmenta diverses manifestacions com la vocal o el paper, no està directament dirigit a la protecció d'informació que es facilita a través d'aquests mitjans.

Els sistemes informàtics de la companyia són únicament per a ús professional. L'ús esporàdic amb finalitats personals es permetrà si l'usuari:

- no consumeix més que una petita quantitat de recursos que podrien ser utilitzats amb finalitats professionals,
- No interfereix en la seva productivitat i,
- No suposi una amenaça per a qualsevol activitat del negoci.

Es consideraria ús personal esporàdic permissible, per exemple, enviar un missatge per programar un esmorzar. Qualsevol altre tipus d'ús personal requereix el permís del cap de departament.

Els jocs integrats en els sistemes operatius dels ordinadors (com Windows de Microsoft) estan permesos, sempre que es jugui durant els descansos, hora del menjar i no interfereixin en la productivitat o motivació dels empleats.

Altres jocs que formin part d'un paquet de programari independentment estan totalment prohibits; així com l'ús dels sistemes informàtics de la companyia per mantenir cadenes de cartes, recerca de donants per a associacions de caritat, material electoral, religiós o un altre ús diferent del relacionat amb el negoci.

9.2.7 Responsabilitats en la Gestió de la Seguretat

9.2.8 Principals departaments responsables de la seguretat de la informació

L'orientació, direcció i autoritat per a les activitats de seguretat informàtica estaran centralitzats per a totes les unitats d'organització de la companyia en el Departament de Seguretat de Tecnologies de la Informació.

Serà responsabilitat del Departament de Seguretat de Tecnologies de la Informació, a nivell de tota l'organització, l'establiment i posterior manteniment i auditoria de la normativa per a la protecció d'informació: pautes, guies i procediments.

Així mateix, el Departament de Seguretat de Tecnologies de la Informació s'encarregarà d'investigar les intrusions en els sistemes i altres incidents relacionats amb la violació de la seguretat.

Les mesures de disciplina resultants d'una violació de la seguretat informàtica seran gestionats per el Departament de Recursos Humans.

9.2.9 Categories de responsabilitat

Amb la finalitat de coordinar l'esforç d'equip del que parlàvem anteriorment, la companyia estableix tres categories, de les quals almenys una es refereix a cadascun dels empleats.

Aquestes categories són les següents: Propietari, Administrador i Usuari. Tals categories defineixen les responsabilitats generals pel que fa a la protecció informàtica.

9.2.10 Responsabilitat dels propietaris

Els Propietaris de la Informació seran els caps de departament, alts directius, o els seus delegats dins de la companyia, a els qui se'ls assignarà la responsabilitat d'adquirir, desenvolupar i mantenir la producció i adquisició d'aplicacions, documents i bases de dades que gestionin la informació de la companyia.

Aquestes aplicacions seran programes que regularment facilitin informes que recolzin la presa de decisions i altres activitats relacionades amb el negoci.

Tota producció d'aplicacions, documents i bases de dades que gestionin la informació tindran un propietari designat. Segons el tipus d'informació, els propietaris classificaran la seva confidencialitat (descrit més endavant), designaran els usuaris als quals se'ls permeti l'accés, i finalment, aprovaran les diverses formes en què la informació serà utilitzada.

9.2.11 Responsabilitat dels administradors

Els Administradors posseeixen de forma física o lògica tant la informació de la companyia, com la qual a aquesta ha estat confiada.

Encara que els membres del Departament de Sistemes són Administradors, els Administradors de sistemes locals també ho són. Sempre que la informació es mantingui exclusivament en un ordinador personal, necessàriament, l'usuari serà també Administrador.

Cada tipus d'aplicació, document o bases de dades del sistema informàtic haurà de tenir un o més Administradors assignats. Els Administradors hauran de salvaguardar la informació, implementar sistemes de control d'accés per prevenir la divulgació d'aquesta

informació de forma inadequada i fer còpies de seguretat perquè mai es perdi informació de valor.

A més, els Administradors hauran d'implementar, operar i mantenir les mesures de seguretat establertes pels propietaris de la informació.

9.2.12 Responsabilitat dels usuaris

Correspon als Usuaris el responsabilitzar-se i complir amb tota la normativa de la companyia, procediments, i estàndards relacionats amb la seguretat informàtica.

Qüestions relacionades amb la gestió apropiada d'un específic tipus d'informació seran dirigides al seu Administrador, o bé al Propietari de la informació en qüestió.

Atès que els sistemes informàtics es distribueixen cada vegada més (a través d'ordinadors personals, portàtils, etc.) els Usuaris progressivament s'adonen de la necessitat de posar en pràctica mesures de seguretat que tal vegada no necessiten conèixer anteriorment.

9.2.13 Maneig consistent de la informació

La informació de la companyia, o que se li ha confiat, s'ha de protegir segons la seva confidencialitat. S'han d'emprar mesures de seguretat independentment del suport en què la informació està emmagatzemada (paper, transparències, bits, etc.), sistema en què es processi (ordinadors personals, tallafocs, bústies de veu, etc.), o mitjà pel qual es mogui (correu electrònic, conversa cara a cara, etc.). La informació s'ha de protegir de forma eficaç, sense tenir en compte el punt en què es trobi en el seu cicle vital, des del seu origen fins a la seva destrucció.

9.2.14 Responsabilitat de les còpies de seguretat

Amb l'objectiu de protegir les fonts d'informació de la companyia de pèrdua, o dany, els usuaris tenen la responsabilitat de fer còpies de seguretat de les dades dels seus ordinadors regularment, bé ells mateixos, o bé, assegurar-se que algú ho fa en el seu lloc.

El responsable de fer periòdicament aquestes còpies per als sistemes de comunicació i ordinadors multiusuari és el Departament de Sistemes. En cas de sol•licitud específica, el Departament de Sistemes instal·larà, o bé facilitarà l'assistència tècnica necessària per a la instal·lació de còpies de seguretat maquinari o programari.

Tota còpia de seguretat que contingui informació confidencial de qualsevol grau estarà encriptada i serà emmagatzemada amb la codificació o controls d'accés físic corresponents, en un lloc aprovat.

S'ha de disposar d'un pla d'emergència per a totes les aplicacions que gestionen informació confidencial, i la responsabilitat de verificar que aquest pla és degudament

desenvolupat, actualitzat i avaluat regularment recau sobre el Propietari de la informació.

9.2.15 Emmagatzematge de la informació

La companyia disposa de servidors de fitxers i bases de dades per emmagatzemar tota la informació.

Queda totalment prohibit sense autorització de direcció i el Departament de Sistemes emmagatzemar qualsevol tipus d'informació de la companyia en els sistemes locals o al nuvol, tota la informació estarà emmagatzemada en els servidors de la companyia..

9.2.16 Classificació de la informació

9.2.16.1 Sistema de classificació

La companyia ha adoptat un sistema de classificació d'informació que la distingeix en quatre grups.

Tota la informació sota control de la companyia, tant si ha estat generada interna o externament es distingirà dins d'aquestes categories: Secreta, Confidencial, Solament per a Ús Intern i Pública.

Tots els empleats hauran de familiaritzar-se amb les definicions d'aquestes categories i amb els procediments a seguir per a la seguretat informàtica segons la categoria a la qual pertanyi.

Segons aquesta Normativa, "informació sensible" és aquella que pertany a la categoria secreta o confidencial.

9.2.16.2 Etiquetatge de la classificació de la informació

En cas que la informació sigui sensible, des del moment en què es crea fins que es destrueix, haurà d'estar etiqueta (marcada) amb la corresponent denominació.

Aquestes marques han d'estar presents en totes les manifestacions de la informació (còpies impreses, disquets, CD-ROMs, etc.).

La major part de la informació de la companyia està dins de la categoria Solament per a Ús Intern. Per això, no és necessari etiquetar la informació que és només per a ús intern. És a dir, la informació sense etiquetar es considerarà informació només d'ús intern.

9.2.17 Control d'accés a la Informació

9.2.17.1 Accés basat en la necessitat del saber

L'accés a la informació que és propietat o sota el control de la companyia es permetrà segons la necessitat de coneixement. En altres paraules, només se'ls permetrà accés a aquells que tinguin una necessitat legítima de tal informació per al negoci.

De la mateixa manera, els empleats no han de retenir l'accés a la informació quan el Propietari de la informació és qüestió doni instruccions de compartir-la. **Per implementar el concepte de Necessitat de Coneixement, la companyia ha adoptat un procés de sol·licitud i aprovació per part del Propietari.**

Els empleats no han d'intentar accedir a la informació confidencial sense la prèvia aprovació de drets de per part del Propietari. **Quan un empleat varia les seves tasques (incloent la finalització de contracte, trasllat, ascens o excedència), el seu supervisor haurà de notificar-ho immediatament al Departament de Seguretat de Tecnologies de la Informació.**

Els privilegis concedits als empleats seran revisats pels Propietaris i Administradors de forma periòdica, per assegurar que solament aquells amb Necessitat de Coneixement tinguin accés a la informació sensible.

9.2.18 Identificadors d'usuari i contrasenyes

Per implementar el procés de Necessitat de Coneixement, la companyia insisteix que cada empleat amb accés als sistemes informàtics multiusuaris tingui un únic nom d'usuari i contrasenya privada.
Aquests noms d'usuari serviran per restringir privilegis basant-se en les tasques del lloc, responsabilitats de projecte i altres activitats del negoci.
Cada empleat és personalment responsable de l'ús del seu nom d'usuari i contrasenya.

9.2.19 Identificadors per a usuaris anònims

Exceptuant els taulers d'anuncis electrònics, les pàgines d'Internet i intranet i altres sistemes els usuaris dels quals són anònims de forma intencionada, es prohibeix l'accés a qualsevol dels sistemes de la companyia, o sistemes en xarxa, de forma anònima.
L'accés anònim podria suposar, per exemple, la utilització d'un nom d'usuari "convidat".
Quan un usuari empra sistemes d'ordres que permeten canviar el nom d'usuari actiu per adquirir certs privilegis, haurà d'haver introduït prèviament el seu nom d'usuari, aquell que clarament indica la seva identitat.

9.2.20 Política de control de les contrasenyes

Les contrasenyes dels comptes d'usuaris són el mecanisme bàsic adoptat per l'organització per a control l'accés a la informació i autenticar els accessos autoritzats pel que hauran de ser especialment cuidat el seu ús i per tant tots els usuaris hauran de complir amb les següents normes.

9.2.20.1 Difícils d'endevinar

Per assegurar que els sistemes de contrasenyes compleixen el paper que es correspon, els usuaris hauran de triar contrasenyes que siguin difícils d'endevinar. Això és, la contrasenya no ha d'estar relacionada amb la vida personal o professional. No hauria de triar-se com a contrasenya, per exemple, el nombre de la matrícula del cotxe, el nom del cònjuge o fragments d'una adreça.
D'altra banda, no podrà ser contrasenya una paraula del diccionari o de qualsevol altre àmbit del parla.
Alguns exemples de paraules que no podrien ser contrasenyes són: noms propis o de llocs, termes tècnics o d'argot.

9.2.20.2 Fàcils de recordar

Els usuaris poden triar contrasenyes que siguin fàcils de recordar i alhora difícils d'endevinar per a persones no autoritzades seguint algun d'aquests mètodes:

- unint diverses paraules,
- movent una paraula cap amunt, a baix, a la dreta o a l'esquerra en la línia corresponent del teclat.
- Saltant un cert nombre de caràcters a dalt o a baix en l'abecedari.
- Transformant una paraula comuna segons un mètode determinat, com canviar per un nombre cada dues lletres reflectint la seva posició en la paraula.
- Combinant una paraula amb signes de puntuació o nombres.
- Formant sigles a partir de paraules en una cançó, poema o una altra seqüència de paraules coneguda.
- Escrivint una paraula incorrecta de forma deliberada. (preferiblement que no es tracti d'un error comú d'ortografia).
- Combinant diverses preferències com a colors o hores de somni.

9.2.20.3 Limitacions

No s'ha de configurar com a contrasenya una seqüència de caràcters parcialment transformada segons la data o un altre factor predictible.
No s'empraran contrasenyes del tipus "X3ENA" al gener, "X34FEB" al febrer, etc. És més, els usuaris no han de formar contrasenyes similars o idèntiques a les quals han emprat anteriorment.
Per dificultar encara més que una contrasenya sigui descoberta, aquesta ha de tenir com a mínim set caràcters. Amb la finalitat d'assegurar que una contrasenya compromesa no s'utilitza de forma inadequada durant llargs períodes de temps, les contrasenyes hauràs de canviar-se cada interval de 45 dies sinó abans.
En el moment en què un empleat sospiti que una altra persona ha descobert una contrasenya, aquesta haurà de ser immediatament canviada i s'haurà de notificar al seu responsable i aquest al departament de seguretat.

9.2.20.4 Emmagatzematge

Les contrasenyes no s'han d'emmagatzemar en cap mitjà llegible com a fitxers de processament per lots, directives, macros de programari, tecles de funció d'un Terminal, ordinadors sense sistemes de control d'accés, o uns altres puguin ser descobertes per persones sense autorització.
De la mateixa manera, les contrasenyes no han d'escriure's de forma alguna que puguin ser desxifrades fàcilment, ni deixar-se en algun lloc on persones sense autorització puguin descobrir-les.
Totes les contrasenyes d'us corporatiu no personals, com credencials per accedir a ftps, webs, banca electrònica, targetes de crèdit, etc.. estaran emmagatzemades i encriptades amb software proporcionat per el Departament de Seguretat de Tecnologies de la Informació, no està permès emmagatzemar aquestes credencials en documents sense encriptar, com podrien ser documents de text, fulls de càlcul i similars.

9.2.21 Compartir

En cas que diversos usuaris necessitin compartir la informació d'un ordinador, hauran d'utilitzar el correu electrònic, bases de dades en programari per a grups, directoris públics de l'àrea local de servidors, i altres mecanismes.

Encara que es comparteixin els noms d'usuari, per exemple, per al correu electrònic, les contrasenyes mai s'han de compartir o revelar a uns altres. Només existeix dos excepcions, les contrasenyes caducades, que es reben en assignar el nom d'usuari i els usuaris compartits, aquests usuaris tendiran a ser suprimits i que tothom tingui credencials personals per accedir al sistema.
S'ha de canviar aquestes contrasenyes la primera vegada que l'usuari amb accés entra en el sistema. La revelació d'una contrasenya (o qualsevol altre mecanisme d'accés com un senyal contrasenya dinàmica) fa a l'usuari amb autorització responsable de les accions que es duguin a terme amb tal contrasenya.
Si un empleat creu que el seu nom d'usuari i contrasenya estan sent utilitzades per algú més, haurà de notificar-ho immediatament a l'administrador de seguretat encarregat del sistema de seguretat en qüestió.

9.2.22 Aspectes relacionats amb el Personal

9.2.22.1 Contracte de seguretat

Tot emprat que desitgi utilitzar els sistemes informàtics multiusuaris de la companyia, ha de signar una declaració de conformitat abans que se li assigni un nom d'usuari.
En cas que ja disposi d'un nom d'usuari, haurà de signar la declaració de conformitat abans de procedir a la renovació del nom d'usuari.
La signatura d'aquesta declaració implica que el signant entén i està d'acord a complir la normativa, de la companyia relacionada amb els ordinadors i sistemes en xarxa (inclusivament les instruccions d'aquesta normativa).

9.2.22.2 Teletreballadors

Sota criteri de la direcció, alguns empleats qualificats podran fer part del seu treball des de casa.
El permís per teletreballar serà concedit pel superior immediat basant-se en una sèrie de factors rellevants.
La renovació del permís per teletreballar depèn en part de la conformitat de certes normatives i estàndards relacionades amb la seguretat informàtica.
L'obertura del correu electrònic des del cotxe, de camí a casa, no es considera teletreball, encara que sí implica que els empleats prenguin moltes de les mateixes precaucions.

9.2.22.3 Protecció contra robatoris

Tots els ordinadors i equips de sistemes en xarxa de la companyia situats en llocs oberts de l'oficina hauran d'estar dotats amb dispositius antirobatori.
Els servidors en xarxa de l'àrea local i altres sistemes multiusuaris se situaran en caixes, armaris o habitacions amb tancaments apropiats. En canvi, els ordinadors portàtils hauran d'assegurar-se mitjançant la utilització de cables de seguretat, situant-los sota clau en caixes, o utilitzant qualsevol altre sistema de tancament que els protegeixi quan estiguin en l'oficina encara que no estiguin en funcionament.
No està permès extreure ni en part, ni íntegrament equips informàtics o entorns de xarxa de la companyia fora dels seus límits físics, sense que la persona en qüestió hagi rebut la corresponent passada de propietat per part de la direcció de l'edifici. Els cerques i els telèfons mòbils no estan inclosos en aquesta normativa.

9.2.22.4 Divulgació d'informació de seguretat

Tota la informació relacionada amb les mesures de seguretat per a ordinadors i sistemes en xarxa de la companyia és confidencial, i per tant, no podrà ser comunicada a aquells

que no siguin usuaris del sistema en qüestió, sense el degut permís del Responsable de Seguretat Informàtica.
Per exemple, està prohibida la publicació en directoris de nombres del telèfon, de mòdems o altres sistemes d'accés. No obstant això, aquesta norma no afecta a les adreces de correu electrònic.

9.2.22.5 Drets sobre els desenvolupaments

Mentre es presti un servei a la companyia, els seus empleats cedeixen exclusivament a aquesta els drets de patents, reproducció i invents o una altra propietat intel·lectual que ells originin i/o desenvolupin.
Tots els programes i documentació generada o facilitada pels empleats per a benefici de la companyia es consideren propietat de la companyia.
La companyia assumeix tots els drets legals de propietat dels continguts de tots els sistemes informàtics sota el seu control (subjecte a prèvia reclamació, per exemple de programari amb drets de còpia llicenciat per tercers). Per tant, la companyia es reserva el dret d'accés i ús de la seva informació.

9.2.22.6 Dret a vigilar i buscar

Amb la finalitat d'assegurar el compliment de la normativa, les lleis i regulacions aplicables i la seguretat dels seus empleats, la companyia es reserva el dret a inspeccionar en qualsevol moment i portar un seguiment de tots els sistemes informàtics de la companyia.
Tal inspecció pot tenir lloc amb o sense el consentiment, coneixement o presència dels empleats implicats.
Els sistemes informàtics subjectes a inspecció inclouen, però no es limiten als arxius de sistema de correu electrònic, arxius del disc dur d'ordinadors personals, arxius de bústia de veu, arxius d'impressores, documentació obtinguda per fax, calaixos de l'escriptori i àrees d'emmagatzemar.
Aquestes inspeccions es duran a terme després **d'haver estat aprovades pels Departaments de Seguretat i Assumptes Legals.**
Atès que els ordinadors i sistemes de la companyia es posen a la disposició dels seus empleats únicament per a ús professional, aquests no han d'esperar respecte algun de privadesa associada amb la informació que s'emmagatzema o envia a través d'aquests sistemes informàtics.
La companyia a més es reserva el dret d'eliminar dels seus sistemes informàtics qualsevol material que consideri ofensiu o potencialment il·legal.

9.2.22.7 Ús personal de la informació.

Els sistemes informàtics de la companyia són únicament per a ús professional. L'ús esporàdic amb finalitats personals es permetrà si l'usuari:

- no consumeix més que una petita quantitat de recursos que podrien ser utilitzats amb finalitats professionals.
- No interfereix en la seva productivitat.
- No suposi una amenaça per a qualsevol activitat de negoci.

Es consideraria ús personal esporàdic permissible, per exemple, enviar un missatge per programar un esmorzar. Qualsevol altre tipus d'ús personal requereix el permís del cap de departament.
Els jocs integrats en els sistemes operatius dels ordinadors (com Windows de Microsoft) estan permesos, sempre que es juguin durant els descansos, hora del menjar i no interfereixin en la productivitat o motivació dels empleats.

Altres jocs que formin part d'un paquet de programari independent estan totalment prohibits; així com l'ús dels sistemes informàtics de la companyia per mantenir cadenes de cartes, recerca de donants per a associacions de caritat, material electoral, religiós o un altre ús diferent del relacionat amb el negoci.

9.2.22.8 Conductes inadequades.

La direcció de la companyia es reserva qualsevol dret a revocar els privilegis de sistemes de qualsevol usuari en qualsevol moment.
No es permetrà conducta alguna que interfereixi amb el ritme habitual i adequat dels sistemes informàtics de la companyia, que impedeixi a uns altres utilitzar aquests sistemes o bé que sigui perillós o ofensiu.

9.2.22.9 Aplicacions que comprometen la seguretat.

Excepte concessió de la corresponent autorització per part del Departament de Seguretat de Tecnologies de la Informació, els empleats de la companyia en cap concepte hauran d'adquirir, posseir, negociar o utilitzar eines de maquinari o programari que poguessin ser emprades per avaluar o comprometre els sistemes de seguretat informàtica.
Alguns exemples d'aquestes eines són aquelles que ignoren la protecció programari contra còpia no autoritzada, detecten contrasenyes secretes, identifiquen punts de seguretat vulnerables i descodifiquen arxius en clau. Així mateix, sense el permís adequat, es prohibeix als empleats utilitzar rastrejadors o un altre tipus de maquinari o programari que detecti tràfic d'un sistema en xarxa o l'activitat d'un ordinador.
Els incidents relacionats amb la pirateria informàtica, descobriment de contrasenyes, descodificació d'arxius, copiant pirateria de programari i altres activitats que suposin una amenaça per a les mesures de seguretat, o siguin il·legals es consideraran violacions greus de la normativa interna de la companyia.
També està terminantment prohibit l'ús de sistemes de bypass, que el seu objectiu és evitar les mesures de protecció i bromes o acudits pràctics que posin en joc els sistemes de protecció.

9.2.22.10 Denúncia obligatòria

Totes les suposades violacions de la normativa, intrusions al sistema, infeccions de virus i altres condicions que suposin, un risc per a la informació o els sistemes informàtics de la companyia, hauran de ser immediatament notificades al Departament de Seguretat Informàtica.
Els usuaris no han de comprovar o intentar comprometre les mesures de seguretat d'un ordinador o sistema de comunicació tret que tal acció hagi estat prèviament aprovada, per escrit, pel Director del Departament de Revisió Interna.
Els incidents relacionats amb la pirateria informàtica, descobriment de contrasenyes, descodificació d'arxius, copiat pirata de programari i altres activitats que suposin una amenaça per a les mesures de seguretat, o siguin il·legals es consideraran violacions greus de la normativa interna de la companyia.
També està terminantment prohibit l'ús de sistemes de bypass, que el seu objectiu és evitar les mesures de protecció i bromes o acudits pràctics que posin en joc els sistemes de protecció.

9.2.23 Control de terceres parts

9.2.23.1 Compartir informació

A excepció que certa informació hagi estat específicament classificada com a pública, tota la informació interna de la companyia ha de ser protegida contra la seva difusió a terceres persones.

Només es permetrà accés a la informació interna de la companyia quan existeixi una necessitat del seu coneixement demostrable, quan s'hagi signat un acord de no-revelar, o quan hagi estat autoritzat expressament pel propietari de la informació de la companyia en qüestió.
En cas de pèrdua o revelació d'informació confidencial a persones no autoritzades o sospitoses d'aquestes accions, s'haurà de notificar immediatament al Propietari de les dades i al Departament de Seguretat Informàtica.

9.2.23.2 Sol·licituds d'informació

Tret que el Propietari de la Informació hagi concedit permís a un empleat per fer pública certa informació, totes les peticions d'informació de la companyia i les seves activitats han de remetre's al Propietari d'aquesta informació.
Tals peticions inclouen formularis, enquestes i entrevistes en premsa, entre altres formularis d'estudi.
Aquesta normativa no s'aplicarà a les dades de venda i màrqueting de la companyia en relació amb els seus productes i serveis, ni tampoc a les trucades al servei tècnic.
En cas que un empleat, en nom de la companyia, rebi informació confidencial de terceres parts, tal recepció estarà precedida pel corresponent formulari de revelació de la companyia degudament signat.

9.2.24 Control de seguretat a la xarxa de dades

9.2.24.1 Connexions internes

Tots els ordinadors de la companyia que conté informació confidencial i que estan connectats a sistemes en xarxa interns de forma permanent o intermitent hauran d'estar dotats amb un sistema de control d'accés amb contrasenya aprovat pel Departament de Seguretat de Tecnologies de la Informació.
Independentment del tipus de connexió en xarxa que es tracti, tots els ordinadors autosuficients que contenen informació confidencial hauran igualment d'emprar un sistema de control d'accés amb contrasenya aprovat.
És recomanable que els altres ordinadors disposin de protectors de pantalla amb contrasenya dotats amb sistemes de funcionament, de manera que després de detectar un determinat període sense activitat, la pantalla es posi en blanc fins que s'introdueixi de nou la contrasenya correcta.
De la mateixa manera, els sistemes multiusuaris de la companyia han d'utilitzar sistemes de tancament que finalitzin automàticament la sessió d'un usuari després d'un temps definit sense detecció d'activitat.

9.2.24.2 Connexions externes

Tota connexió al sistema de la companyia provinent de l'exterior (Internet, línies telefòniques públiques, etc.) haurà d'estar protegida per un sistema de control d'accés amb una contrasenya dinàmica aprovada.

Les contrasenyes dinàmiques són diferents cada vegada que s'utilitzen, i per tant no poden ser repetides amb la finalitat d'evitar el control d'accés.
Està terminantment prohibit que els usuaris amb ordinadors personals connectats a sistemes en xarxa externs deixin les connexions VPN o altres en funcionament desatesos, mentre el programari de comunicació informàtic està actiu, tret que es tingui instal·lat un sistema de contrasenya dinàmica.
En termes generals, els empleats de la companyia no hauran d'establir connexions amb sistemes en xarxa externs (inclusivament el Servei de Proveïdors d'Internet), sense que

aquestes connexions hagin estat aprovades pel Departament de Seguretat Tecnologies de la Informació.

En cap cas, excepte amb autorització expressa del responsable de Seguretat de Tecnologies de la Informació, és permet connectar cap ordinador, disc dur extern, disc dur intern, o qualsevol sistema en xarxa o dispositiu electrònic sense l'autorització del Departament de Seguretat de Tecnologies de la Informació.

9.2.24.3 Canvis

En els canvis del sistema en xarxa intern de la companyia s'inclouen: instal·lació d'un nou programari de comunicacions, canvi d'adreces del sistema en xarxa, reconfiguració de rutes, incorporació de línies telefòniques, etc.
A excepció de les situacions d'emergència tots els canvis en els sistemes en xarxa de la companyia hauran de ser:

- documentats en un formulari de sol·licitud
- prèviament aprovats pel Departament de Tecnologies de la Informació

Tots els canvis d'emergència en els sistemes en xarxa de la companyia seran exclusivament realitzats per persones autoritzades pel Departament de Tecnologies de la Informació.
L'objectiu d'aquest procés és prevenir canvis inesperats, que de forma inadvertida porten a un bloqueig del servei, la difusió no autoritzada d'informació i altres problemes.
Aquest procés no només afecta als "empleats" segons està detallat en la secció de definicions d'aquesta normativa, sinó també als comercials.

9.2.24.4 Accessos a Internet

Normalment, als treballadors se'ls facilita l'accés a Internet per realitzar les tasques del seu treball. No obstant això, aquest accés pot ser denegat en qualsevol moment si el supervisor de l'empleat en qüestió ho considera oportú.
L'accés a Internet es controla amb la finalitat d'assegurar que els empleats no contactin amb pàgines web que no tinguin relació alguna amb el seu treball, i cerciorar que es compleixen les normatives de seguretat.
En cap cas, excepte amb autorització expressa del responsable de seguretat informàtica, és permet connectar cap dels dispositius de la companyia a cap sistema sense fils (Wi-Fi, Bluetooth, etc...).
Els empleats no han de representar a la companyia en una discussió en grup en Internet o altres fòrums públics, almenys que prèviament hagin rebut un permís de la direcció general.
Així mateix, els empleats no dipositaran material de la companyia (programari, comunicats interns, notes de premsa, bases de dades, etc.) en cap sistema informàtic d'accés públic com a Internet, tret que tal acció hagi estat prèviament aprovada tant pel Propietari de la Informació com pel director del Departament de Tecnologies de la Informació.
L'establiment de pàgines web es gestiona de forma independent per un procés d'aprovació en el qual està implicat el Comitè de Comunicacions Externes.
De la mateixa manera, es prohibeix establir acords comercials electrònics a través d'Internet sense la corresponent avaluació i aprovació dels departaments de Tecnologies de la Informació i de Seguretat Informàtica.
D'altra banda i sempre que sigui possible, mai s'enviarà informació confidencial, via Internet, que no estigui xifrada o codificada.

Correu electrònic:

- No utilitzar l'adreça electrònica de la companyia per donar-se d'alta a llocs web o serveis que no estiguin relacionats amb l'activitat laboral.
- No confiar en correus electrònics de dubtosa procedència.
- No obrir documents adjunts sense comprovar el remitent i el contingut del missatge.
- No enviar informació sensible o confidencial mitjançant el correu electrònic, sinó és estrictament necessari.

Navegació web:

- No accedir a llocs webs o continguts no relacionats amb l'àmbit laboral.
- No descarregar aplicacions ni continguts de dubtosa procedència.
- Per la tramitació o l'enviament d'informació sensible utilitzar sempre el protocol https.

9.2.25 Control contra programari maliciós

9.2.25.1 Localització

En l'actualitat, els virus poden dispersar-se fàcilment no només en els arxius de programa, sinó també en els arxius de dades.
Dins dels símptomes d'infecció de virus, es troben un temps de resposta més lent, pèrdua inexplicable d'arxius, canvi de dates d'arxius, augment de la grandària dels arxius i fallada total dels ordinadors personals i servidors.
Amb la finalitat d'assegurar un servei continuat tant per als ordinadors, com per als sistemes en xarxa, tots els usuaris d'ordinadors personals hauran de tenir una versió actualitzada del programari antivirus aprovat instal·lat en els seus ordinadors.
Aquests sistemes de detecció de virus s'han d'emprar per comprovar tots els arxius i programari que provenen tant de terceres persones com d'altres grups dins de la companyia.
La comprovació pertinent haurà de realitzar-se abans d'obrir els arxius o executar el programari. Els empleats mai hauran de saltar-se o apagar aquests sistemes, donat el perill d'infecció de virus.

9.2.25.2 Eliminació

Si un empleat sospita d'infecció de virus, immediatament ha de deixar d'utilitzar l'ordinador en qüestió i posar-se en contacte amb el lloc d'ajuda. A més, l'ordinador haurà de ser aïllat dels sistemes en xarxa.
Els disquets i altres mitjans magnètics d'emmagatzematge que hagin estat utilitzats en l'ordinador infectat no han de ser utilitzats en cap altre ordinador fins que el virus hagi estat satisfactòriament eliminat.
Els usuaris mai intentaran eliminar el virus per si mateixos. Sinó que s'avisarà als empleats de la companyia degudament qualificats per realitzar aquesta tasca de forma eficaç reduint al màxim tant la destrucció d'informació com el temps de caiguda del sistema.

9.2.25.3 Còpies de seguretat netes de virus

Per procedir a la restauració de les activitats habituals d'un ordinador personal després d'infecció de virus, tot el programari ha de ser copiat abans d'iniciar la seva utilització, i aquestes còpies hauran de ser degudament emmagatzemades en un lloc segur.
La còpia mestra, en lloc de ser utilitzada per a activitats ordinàries del negoci, es reservarà per ser recuperada després d'infecció de virus, caiguda del disc dur i altres problemes.

9.2.25.4 Fonts autoritzades d'aplicacions

Els grans sistemes d'ordinadors generalment no sofreixen de virus, però en canvi es veuen afectats per cucs, cavalls de troià i ransomware.
Els cucs són similars als virus, solament que no s'adjunten a altres programes. Els cavalls troià són programes no autoritzats amagats dins de programes autoritzats. Els ransomwares són un tipus de programes informàtics malintencionats que restringeixen l'accés a determinades parts o arxius del sistema infectat, i demana un rescat a canvi de llevar aquesta restricció
Per evitar problemes amb virus, cucs, cavalls de troians, ransomware i qualsevol tipus de malware, els ordinadors i sistemes en xarxa de la companyia mai executaran programari que procedeixi d'una altra font diferent de:

- un altre departament de la companyia
- grups d'usuaris coneguts i fiables
- les mateixes autoritats en sistemes de seguretat
- proveïdors establerts d'ordinadors o sistemes de xarxa.

En cap concepte s'utilitzarà programari obtingut dels taulons de notícies electrònics, programari compartit, programari de domini públic, i un altre programari procedent de fonts que no siguin d'absoluta fiabilitat, tret que hagi estat prèviament avaluat i aprovat pel Departament de Seguretat Informàtica

9.2.26 Controls en el procés de desenvolupament de programari

9.2.26.1 Especificacions escrites

Tot programari desenvolupat per personal intern o extern i dissenyat per processar informació de diversa confidencialitat de la companyia deurà rebre l'especificació formal per escrit corresponent.
Aquesta especificació inclourà una relació tant de riscos com de controls de seguretat (incloent accés als sistemes de seguretat i plans d'emergència).
L'especificació ha de formar part d'un acord entre el Propietari Informàtic implicat i l'encarregat del desenvolupament del sistema. A l'efecte d'aquest paràgraf, els macros dels fulls de càlcul, i documents de processadors de text no es consideren programari.

9.2.26.2 Aprovació del departament de Seguretat de Tecnologies de la Informació

Prèvia utilització, els sistemes d'aplicacions nous o, en certa mesura transformats han de rebre la corresponent aprovació del Departament de Seguretat de Tecnologies de la Informació per escrit.
Aquest requisit afecta als ordinadors personals tant com als grans sistemes.

9.2.26.3 Control de canvis

TIPUS DE PROCÉS	**JERARQUIA DEL PROCÉS**
☐Estratègic ☐ Fonamental ☒ Suport	✓ Procés o processos superiors: No aplica ✓ Processos del mateix nivell amb els que està relacionat: - Desenvolupament, revisió i millora del SGSI - Revisió per la Direcció - Gestió d'incidències i No Conformitats ✓ Procés inferior: No aplica

Tots els sistemes de comunicacions i ordinadors que s'usen en la companyia empraran un control documentat del procés de canvis que asseguri que només es realitzen canvis autoritzats.
Aquest procediment de control de canvi s'ha d'emprar para tots els canvis significatius realitzats al programari del sistema de producció, maquinari, enllaços i procediments de comunicacions.
De nou, aquesta normativa s'aplicarà als ordinadors personals encarregats dels sistemes de producció de la mateixa manera que als sistemes multiusuaris una miqueta majors.

9.2.26.4 Manera d'abordar el desenvolupament de sistemes

Tota activitat de producció, desenvolupament i manteniment de programari dut a terme per empleats de la companyia han de complir amb els estàndards, procediments i altres normatives del Departament de Seguretat de Tecnologies de la Informació.
Entre uns altres, aquests estàndards inclouen els procediments d'avaluació, formació i documentació adequats.

9.2.26.5 Llicències adequades

La companyia produeix un nombre de còpies de programari amb llicència que permeti als seus empleats fer el seu treball de forma convenient i eficient.
Quan es doni el cas que còpies addicionals siguin necessàries per al negoci, la direcció de la companyia haurà d'arribar als acords oportuns amb els proveïdors.
Amb la finalitat d'assegurar la compatibilitat del nou programari amb els ordinadors i sistemes en xarxa de la companyia i per facilitar a la direcció el control de llicències totes les ordres de compra es realitzaran a través del Departament de compres.

9.2.26.6 Còpies no autoritzades

En cap concepte els usuaris hauran de copiar el programari facilitat per la companyia en tipus algun de suport informàtic (disquet, cinta magnètica, etc), transferit a un altre ordinador o lliurar-ho a tercers sense el corresponent permís del supervisor.
Les còpies de seguretat són l'excepció a aquesta norma, ja que no segueixen estrictament els requisits d'autorització.

9.3 Annex 3 (procediment d'auditories Internes)

ELABORAT	**REVISAT**	**APROVAT**
25/03/2019 Departament de Qualitat		

Departament Seguretat Informatica		

ÍNDEX

CONTROL DE MODIFICACIONS

DATA	NUM. EDICIÓ	MOTIU DEL CANVI
30/03/2016	01	S'ha incorporat la definició d'auditoria energètica i el seu objectiu
06/06/2018	02	Es modifica la referència a la normativa UNE.

1. OBJECTE

Aquest procés té per objectiu establir la sistemàtica per planificar, realitzar i documentar els resultats de les auditories internes del sistema de gestió de seguretat de la informació (en endavant SGSI).

Les auditories tenen per objecte verificar el grau de compliment i eficàcia del SGSI implantat, definit en els documents del SGSI i evidenciat en els registres generats.

2. ÀMBIT

Aquest procediment és d'aplicació a tots els processos de l'organització.

3. DOCUMENTACIÓ DE REFERÈNCIA

Norma UNE- EN ISO 9001:2015
Norma UNE-EN ISO 14001:2015
Norma UNE-EN ISO 50001:2011
Norma UNE-EN ISO/IEC 27001
Norma UNE-EN ISO/IEC 27002

4. RESPONSABILITATS

Responsable del SGSI
Establir la proposta d'auditories del SGSI i fer-ne el seguiment
Realització de les auditories internes o delegació de la tasca

Directora de Qualitat i Director d'Operacions
Anàlisi del resultat de les auditories

5. DESENVOLUPAMENT

5.1. Tipologia de les auditories

Els tipus d'auditoria que es troben definits per part de l'organització es corresponen a:

Auditories del Sistema de Gestió de seguretat de la Informació: tenen per finalitat dur a terme una revisió de tots els processos que afecten a l'organització.

Auditories de procés: auditories específiques d'un procés determinat per tal de comprovar la seva eficiència.

Auditoria energètica: diagnosi energètica que té per objectiu l'avaluació del compliment dels objectius energètics.

5.2. Planificació de les auditories

El Responsable del **Sistema de Gestió de seguretat de la Informació** elabora, anualment, el Programa d'auditories del Sistema i les auditories de procés.

Estableix les dates previstes per la realització de les auditories, el procés o processos a auditar i l'equip auditor que la portarà a terme. La programació de les auditories assegura que totes les àrees de l'organització són auditades almenys una vegada a l'any.

Direcció General du a terme l'aprovació dels Plans d'Auditoria.

5.3. Selecció de l'equip auditor

Desde Direcció General es selecciona i contracta l'equip auditor en cas que sigui necessari.

La(es) persona(es) designada(es) com a auditor(es), ha de disposar de formació professional adequada i complir amb els requisits següents:

- Formació específica en auditories (teòrica i pràctica).
- Tenir coneixements específics en **Sistema de Gestió de seguretat de la Informació**.
- Disposar d'experiència o formació demostrable en els processos a auditar

La formació i coneixements de l'auditor s'evidenciarà amb l'entrega del certificat de formació corresponent i/o el currículum.

5.4. Realització de les auditories

5.4.1. Auditories del Sistema de Gestió de seguretat de la Informació

La realització de les auditories es desenvolupa en les següents etapes:

Preparació de l'auditoria

Amb una antelació mínima d'una setmana sobre la data prevista, l'equip auditor enviarà el Pla d'Auditoria al Responsable del **Sistema de Gestió de seguretat de la Informació** o Responsable del Departament afectat (Director i/o Cap del/s Departament/s).

Reunió inicial

L'auditoria comença amb una reunió inicial entre l'auditor i el Director General o persona/es delegada/es. La finalitat d'aquesta etapa es preveure el temps d'auditoria, els elements a auditar i les entrevistes que es realitzaran, prenent com a referència el que descriu el Pla de l'auditoria.

Desenvolupament de l'auditoria

L'auditor en l'exercici de les seves funcions, entrevista als responsables de l'execució de les activitats, examina la documentació i els registres generats, i ratifica la informació rebuda amb visites a les instal·lacions verificant que es compleixen els requisits definits al SGSI o en el marc de treball a auditar. El personal auditat facilita tota la informació sol·licitada i col·labora per a la correcta realització de l'auditoria.

El treball de l'equip auditor consisteix en detectar desviacions dels requisits especificats. Les desviacions han de ser contrastades per evidències objectives.

Reunió final

L'equip auditor, abans d'elaborar l'informe d'auditoria té una reunió amb el Director General o persones delegades i amb els responsables de les funcions afectades, per presentar les desviacions, observacions i recomanacions de l'auditoria, de manera que s'asseguri que s'entenen clarament els resultats de l'auditoria.

5.4.2 Auditories de procés

El procediment de realitzar les auditories és el següent:

1) Informar al Cap/Director del Departament afectat per si aquest considera que ha d'estar present durant la realització de l'auditoria

2) Seguiment del checklist d'auditoria per tal de deixar per escrit les evidències corresponents a través del 01-RS03 Check list d'auditoria
3) Revisió dels punts i comunicació dels resultats al Cap/ Director del Departament.

El mateix Cap de Departament pot sol·licitar al Departament de Qualitat l'execució d'una auditoria. El procés a realitzar és a través de l'aplicació kmkey.

5.5. Resultats de les auditories

L'Auditor elabora l'Informe de l'auditoria. L'equip auditor signa l'Informe d'auditoria i el tramet al Responsable del Sistema de Gestió Integrat el quan n'envia una còpia als diferents responsables dels Departaments Auditats. Opcionalment, l'auditor entrega la llista de comprovació i/o notes de l'auditor.

El Responsable del Sistema de Gestió Integrates responsabilitza de dur a terme el seguiment de les accions correctives necessàries per corregir o eliminar les causes de no conformitats detectades en el transcurs de l'auditoria. Les no conformitats es registraran segons el descrit a la fitxa de procés PS04 Gestió d'incidències i No conformitats.

5.6. Avaluació de les auditories

Direcció General avaluarà la satisfacció del servei realitzat per part de l'equip auditor en el marc de la Revisió per la direcció del Sistema de Gestió de la Qualitat.

6. REGISTRES DEL PROCÉS

- 01-RS03 Llistat de comprovació d'auditoria
- Pla d'Auditoria
- Informe d'auditoria

7. FLUXGRAMA DE PROCÉS

No aplica

9.4 Annex 4 - Gestió d'indicadors

10 Introducció.

La norma ISO27004 en dona una guia per a la mesura dels resultats d'un sistema de gestió de la seguretat de la informació (SGSI) basat en la ISO 27001.

Especifica el sistema de mesura, quan i com mesurar-los.

Ajuda a les empreses a establir objectius relacionats amb el rendiment i els criteris d'èxit. El tipus de mètodes requerits per ISO 27004 depenen de la complexitat, la mida de l'organització,

el cercle entre el cost i el benefici i l'avantatge nivell d'integració de la seguretat de la informació que es trobi en els procediments portats a terme per l'organització.

Aquesta norma especifica com ha de constituir aquests mètodes i com s'hauran d'integrar i documentar les dades assolides en el SGSI.

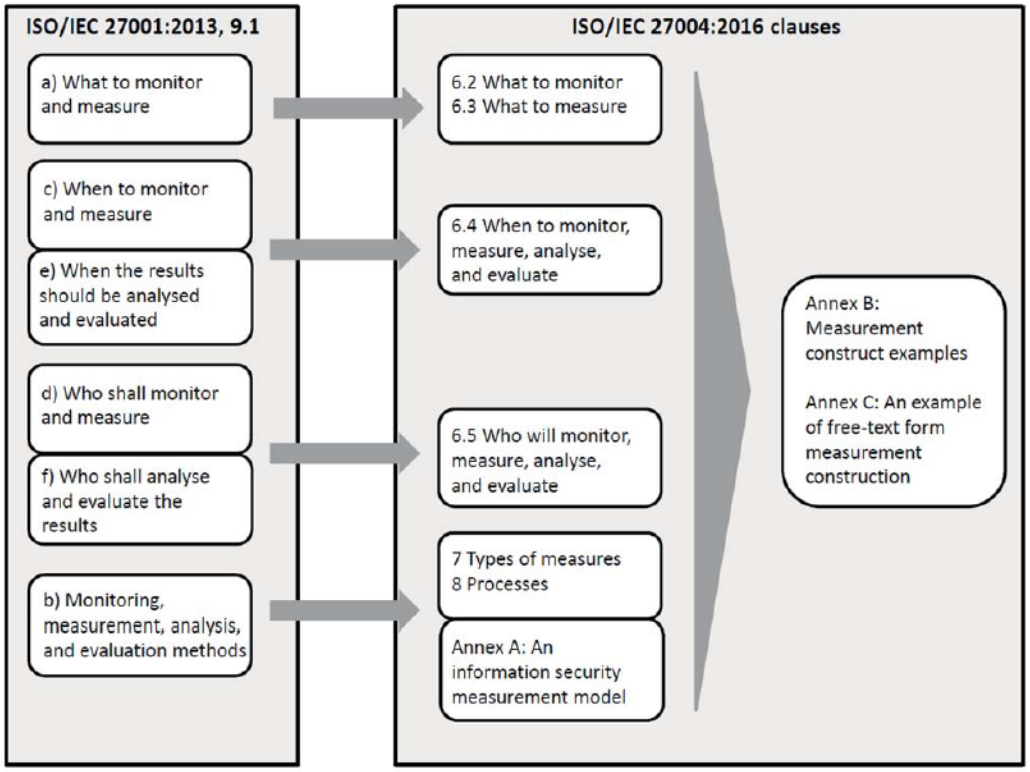


Figure 1 — Mapping to ISO/IEC 27001:2013, 9.1 requirements

11 Objectius.

Els indicadors ens ajudaran a mesurar o avaluar l'eficiència o l'eficàcia dels components implementats en un SGSI.

En definitiva avaluar la seguretat de la informació de la companyia.

12 Fases

Podem dividir la gestió d'indicadors en les següents fases.

- L'elecció dels objectius i processos de mesura
- Descripció de les línies principals: Els valors principals que exposen el punt de referència per a la determinació de cada objecte que està fent-se.
- Selecció de dades: les dades de precisió, oportunitats i dimensions. Es poden dur a terme tècniques de cap programades de recopilació de dades per aconseguir una recopilació normalitzada i mostrar informes.
- Desenvolupar un sistema de mesura: La seqüencia racional d'operacions segons la norma ISO27004 s'aplica en atributs diferents de l'objecte escollit per a la mesura.
- Interpretació i l'anàlisi .

- Notificació dels valors de mesura a les parts interessades.

13 Indicadors.

Tot indicador està compost per:

- Nom.
- Descripció.
- Control de seguretat.
- Formula de mesura.
- Unitat de mesura.
- Freqüència de la mesura.
- Objectiu i llindar.
- Responsable.

13.1 Tipus d'indicadors.

13.1.1 Mesures de rendiment:

Mesures que expressin els resultats previstos en funció de les característiques de l'activitat planejada, com ara el recompte de capçaleres, el compliment de la fita o el grau en què s'han implementat els controls de seguretat de la informació.

Les mesures de rendiment es poden utilitzar per demostrar els progressos en la implementació de processos ISMS, procediments associats i controls de seguretat específics.

13.1.2 Mesures d'eficàcia:

mesures que expressin l'efecte de la realització de les activitats previstes té els objectius de seguretat de la informació de l'organització.

L'efectivitat es refereix a la mesura en què s'han realitzat les activitats previstes i els resultats obtinguts, és a dir descriu l'eficàcia i l'impacte que tenen els processos del SGSI.

13.2 Annex 5 - Procediment de Revisió per Direcció

14 Introducció.

Aquest document descriu les revisións que duran a terme l'equip directiu sobre el pla director de seguretat o SGSI.

15 Periodicitat

Es farà una revisió semestral de l'estat del SGSI, es realitzarà posteriorment a l'auditoria interna.

16 Registre.

En les revisions semestrals es registrarà:

- Lloc
- Assistents.
- Data
- Hora

17 Objectius.

En aquestes revisions l'equip directiu analitzarà:

- Resultats auditories
- Estat dels plans de tractament de risc.
- Resultats dels indicadors definits.
- Procediments dels SGSI.
- Possible punts de millora del SGSI.
- Estat actual del SGSI.
- Formació rebuda pels empleats i estat de maduresa d'aquests.

17.1 Annex 6 - Gestió de Rols i Responsabilitats

1. Introducció.

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, ha d'estar compost almenys per una persona de Direcció, perquè d'aquesta manera les decisions que es prenguin puguin estar recolzades per algun directiu encarregat.

Aquestes responsabilitats i rols es detallen a continuació:

2. Rols i responsabilitats.

El Comitè de Seguretat Informàtica, compost pel director financer com a membre de alta direcció, el cap de sistemes, el responsable d'infraestructures, el cap de qualitat i un membre del departament jurídic.

Aquest Comitè està encarregat d'elaborar i actualitzar les polítiques, normes, pautes i procediments relatius a seguretat de la informació.
A més, és responsable de coordinar l'anàlisi de riscos, plans de contingència i prevenció de desastres.
Cal que durant les reunions trimestrals o segons cronograma, el Comitè efectuarà l'avaluació i revisió de la situació pel que fa a la seva Seguretat de la Informació i Informàtica, incloent l'anàlisi d'incidents ocorreguts que afectin el sistema de la seguretat.
El cap de Recursos Humans, és completament responsable de posar al tant o avisar al personal de les obligacions respecte del compliment de la Política de Seguretat de la Informació.
El cap d'informàtica exercirà les funcions com a responsable de seguretat (RSI) i ha de coordinar i controlar les mesures de seguretat de la informació en qualsevol de les seves formes i en tot el cicle de vida de la Informació, ha d'implantar les directrius de seguretat de la Informació, elaborar i mantenir la política de Seguretat de la Informació i proposar objectius en matèria de seguretat.
El director financer juntament amb el RSI defineix les polítiques, normes, procediments i s'encarrega de fer-les complir. Implanta els controls de seguretat, les accions de correcció i gestiona les vulnerabilitats que es detecten.

3. La seguretat com un treball en equip.

Perquè la seguretat de la informació sigui efectiva, s'ha de dur a terme com una tasca en equip. Aquesta tasca requereix la participació i el suport de cadascun dels empleats de la companyia que tinguin accés a la informació i/o als sistemes informàtics.

D'acord amb tal necessitat de realitzar aquesta tasca com a part del treball d'equip, la present normativa aclareix les responsabilitats dels usuaris, així com els passos a seguir per protegir la informació de la companyia i els seus sistemes informàtics.

4. Persones involucrades

Tot treballador de la companyia, independentment de la seva posició (empleat, contractista, assessor, treballador temporal, etc.), ha de complir amb la normativa per a la seguretat d'informació descrita en aquest i successius documents relacionats amb la seguretat informàtica.

Aquells empleats que violin aquesta o altres normatives per a la seguretat del sistemes i la protecció de la informació estaran subjectes a les corresponents accions disciplinàries, arribant fins i tot a l'acomiadament.

17.2 Annex 7 - Metodologia de Anàlisis de Riscos

1. Metodología a utilizar.

La metodologia que predetermina l'enfocament de l'anàlisi i els criteris de gestió de riscos en el SGSI és Magerit (Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació) i la norma ISO / IEC 27005: 2008.

Primer és necessari definir una fórmula per al càlcul del nivell de risc.

Una vegada establerta aquesta fórmula, defineix els valors que es poden assignar a cadascun dels paràmetres, i elabora una taula de valors.

Exemple: Si l'Impacte = x, la probabilitat és Z llavors el risc és …..

Per calcular el nivell de risc es necessita una fórmula, la qual ha de tenir en compte 3 aspectes fonamentals:

- Confidencialitat
- Integritat
- Disponibilitat

2. Valoració de la pèrdua de Confidencialitat, Integritat o Disponibilitat del Actiu

Cada actiu serà valorat en funció de la criticitat que tingui aquest actiu per a l'organització, tenint en compte, el nivell de protecció que requereix per mantenir la integritat, confidencialitat i disponibilitat de la informació.

Alta. L'actiu intervé en processos crítics per a l'organització (aquells que són necessaris i suficients) i la seva no disponibilitat pot posar en perill la continuïtat del negoci o conté informació amb implicacions legals. **Factor de criticitat: 1**

Mitjana. L'actiu intervé en processos de suport a l'organització. La seva indisponibilitat pot retardar un determinat procés però no es veuria afectada la continuïtat de negoci. **Factor de criticitat: 0,5**

Baixa. L'actiu intervé en processos que no estan directament relacionats amb el negoci, encara que són necessaris. La seva indisponibilitat causa algun contratemps però en cap cas es veuria afectada la continuïtat del negoci. **Factor de criticitat: 0.25**

Molt Baixa: El valor del actiu és pràcticament nul, o bé per la seva baixa incidència, o bé pel baix cost de substitució. **Factor de criticitat: 0,1.**

Nul. El valor del actiu és nul. **Factor de criticitat: 0.**

VALORACIÓ DE LA PERDUA DEL ACTIU

DESCRIPCIÓ	FACTOR CRITICITAT
MOLT CRITIC	1,5
CRITIC	1,25
MOLT ALT	1
ALT	0,75
MITJÀ	0,5
BAIX	0.25
MOLT BAIX	0,1
NUL	0

Quan valorem la pèrdua de cada actiu ho farem dels tres pilars:

- Confidencialitat
- Integritat
- Disponibilitat

I ens quedarem amb el valor més alt.

Per exemple el valor d'un actius és:

ACTIU 1	
PILAR	VALOR
CONFIDENCIALITAT	MOLT ALT
INTEGRITAT	ALT
DISPONIBILITAT	MITJÀ

El valor que ens quedaríem per utilitzar a la formula seria MOLT ALT **Factor Criticitat: 1.**

3. Probabilitat que una amenaça es materialitzi.

PROBABILITAT AMENACES				
ID	DESCRIPCIÓ	PERCENTATGE	VALOR	DESCRIPCIO
6	MOLT ALTA	100	1	GAIREBÉ DIARIAMENT
3	ALTA	75%	0,75	MENSUALMENT
2	MITJA	50%	0,5	UNA VEGADA CADA 6 MESOS
1	BAIXA	25%	0,25	UNA VEGADA AL ANY
	MOLT BAIXA	10%	0,1	UNA VEGADA CADA 5 ANYS

0	**NULL**	0	0	MAI

MOTIVACIÓ AMENACES		
ID	**MOTIVACIO**	**DESCRICPIO**
	NO APLICA	NA
	BAIXA	motivada per joc o demostració de coneixement (B).
	MITJA	amb la intenció de fer un dany a l'empresa (M).
	ALTA	S'intenta obtenció de benefici econòmic o danys a persones (A).

Un cop definits aquests dos factors, la valoració de la capacitat de l'amenaça es fa considerant que l'existència de motivació augmenta el nivell de probabilitat, seguint el següent esquema:

		PROBABILITAT FINAL AMENACES					
		NULL	**MOLT BAIXA**	**BAIXA**	**MITJA**	**ALTA**	**MOLT ALTA**
MOTIVACIO	**NULL**	**NULL**	**MOLT BAIXA**	**BAIXA**	**MITJA**	**ALTA**	**MOLT ALTA**
	BAIX	**NULL**	**MOLT BAIXA**	**BAIXA**	**MITJA**	**ALTA**	**MOLT ALTA**
	MITJÀ	**NULL**	**BAIXA**	**MITJA**	**ALTA**	**ALTA**	**MOLT ALTA**
	ALT	NULL	**NULL**	**MITJA**	**ALTA**	**MOLT ALTA**	**MOLT ALTA**

4. Impacte en l'Organització resultant de la materialització d'una amenaça.

En funció de les conseqüències, s'establiran els següents nivells d'impacte:

Alt. La vulnerabilitat explotada pot provocar l'incompliment d'un requisit legal o danys a persones. El resultat de l'amenaça provoca la visualització de la informació i la seva pèrdua de confidencialitat, afecta no només als processos crítics de l'organització sinó també a la seva missió o la seva imatge exterior. **És quantificada com 100.**

Mitjà. La vulnerabilitat explotada pot provocar un cost per la pèrdua d'actius o la pèrdua de la integritat de la informació, afectant a l'operativa o al negoci de l'organització. **És quantificada com 50.**

Baix. L'exercici de la vulnerabilitat pot provocar la interrupció del sistema o la pèrdua d'algun actiu de poc valor. **És quantificada com 10.**

Nul. L'impacte provocat per l'amenaça és pràcticament nul, o bé per la seva baixa incidència, o bé pel baix cost de substitució. **És quantificada com 0.**

VALOR IMPACTES		
ID	**DESCRIPCIO**	**VALOR**
4	**ALT**	100
3	**MITJÀ**	50
2	**BAIX**	10
0	**NULL**	0

5. Càlcul del Risc.

El risc serà el resultat de creuar la probabilitat que una amenaça pugui actuar sobre una vulnerabilitat, amb l'impacte que pot provocar aquesta amenaça sobre l'actiu, per a això es multiplica el valor de la probabilitat de l'amenaça pel valor de l'impacte.

El resultat d'aquesta multiplicació es pot agrupar en els següents rangs de puntuació:

Risc molt Alt El valor total és major o igual a 75.

Risc Alt. El valor total es troba entre 45 i 74.

Risc Mitjà. El valor total es troba entre 31 i 44.

Risc Baix. El valor total es troba entre 11 i 30.

Risc molt Baix. El valor total és menor o igual a 10.

Risc Null. El valor del risc es 0.

El nivell de risc de cada amenaça serà ponderat en funció de la criticitat de cada actiu, segons l'explicat en la "Identificació o Valoració d'Actius".

Importància molt critica. El risc és multiplicat per 1,5.

Importància critica. El risc és multiplicat per 1,25.

Importància molt alta. El risc és multiplicat per 1.

Importància alta. El risc és multiplicat per 0,75.

Importància Mitjana. El risc és multiplicat per 0,5.

Importància Baixa. El risc és multiplicat per 0,25.

Importància molt baixa. El risc es multiplicat per 0,1.

Sense Importància, El risc es multiplicat per 0.

Risc=Probabilitat x impacte x Criticitat del Actiu

Un cop aplicada aquesta ponderació, es pot determinar el risc total que suporta cada actiu, sumant el valor del Risc Ponderat de totes les amenaces que tenen relació sobre aquest actiu.

De la mateixa manera es pot calcular el valor del Risc per Amenaça, sumant el valor del Risc Ponderat de tots els actius relacionats amb aquesta amenaça.

A partir d'aquesta informació ja es pot iniciar la fase de Gestió del Risc.

17.3 Annex 8.1 - Declaració de Aplicabilitat

17.4 Annex 9.1 - Anàlisi de Riscos

18 Estat del risc: Identificació i valoració.

18.1 Introducció i explicació del càlcul del risc.

Al haver molts actius aquest primer anàlisi es farà tenint en compte la família del actiu per tant primer s'ha definit quines amenaces apliquen a les famílies també està a la fulla de càlcul a la "Creuament Tipus Actiu Amenaces".

18.2 Amenaces.

A cada amenaça se li assigna un impacte i una probabilitat, així per cada amenaça es sap el seu propi risc (Factor Probabilitat * Factor Impacte"), al definir la probabilitat s'ha tingut en compte la motivació.

Amenaça	Origen	Motivació	IMPACTE	PROBABILITAT
Foc	NATURALS	NO APLICA	ALT	BAIXA
Danys per aigua	NATURALS	NO APLICA	ALT	BAIXA
Desastres naturals	NATURALS	NO APLICA	ALT	MOLT BAIXA
Fuga d'informació	HUMANA	ALTA	ALT	MITJA
Introducció de falsa informació	HUMANA	ALTA	ALT	MITJA
Alteració de la informació	ENTORN/ACCIDENTS	ALTA	ALT	MITJA
Corrupció de la informació	ENTORN/ACCIDENTS	NO APLICA	ALT	ALTA

Destrucció de informació	ENTORN/ACCIDENTS	MITJA	ALT	MITJA
Intercepció d'informació (escolta)	HUMANA	MITJA	ALT	MITJA
Tallada del subministrament elèctric	ENTORN/ACCIDENTS	MITJA	ALT	MITJA
Condicions inadequades de temperatura o humitat	ENTORN/ACCIDENTS	MITJA	ALT	ALTA
Fallada de serveis de comunicacions	ENTORN/ACCIDENTS	NO APLICA	ALT	MITJA
Interrupció d'altres serveis i subministres essencials.	ENTORN/ACCIDENTS	NO APLICA	MITJÀ	MITJA
Desastres industrials	ENTORN/ACCIDENTS	NO APLICA	ALT	BAIXA
Malfuncionament dels equips	ENTORN/ACCIDENTS	NO APLICA	ALT	MITJA
Degradació dels suports d'emmagatzematge de la informació	ENTORN/ACCIDENTS	NO APLICA	ALT	BAIXA
Difusió de malware	HUMANA	ALTA	ALT	MITJA
Errors de manteniment / actualització de programes (software)	HUMANA	NO APLICA	ALT	ALTA
Errors de manteniment / actualització d'equips (hardware)	HUMANA	BAIXA	ALT	MITJA
Caiguda del sistema per sobrecarrega	HUMANA	NO APLICA	ALT	BAIXA
Pèrdua d'equips	HUMANA	NO APLICA	ALT	BAIXA
Indisponiblitat del personal	HUMANA	NO APLICA	MITJÀ	MITJA
Abús de privilegis d'accés	HUMANA	ALTA	ALT	MITJA
Accés no autoritzat	HUMANA	ALTA	ALT	MITJA
Errors d'usuaris	HUMANA	NO APLICA	MITJÀ	ALTA
Errors de l'administrador	HUMANA	NO APLICA	ALT	MITJA
Errors de configuració	HUMANA	NO APLICA	ALT	ALTA
Denegació de servei	HUMANA	NO APLICA	ALT	BAIXA
Robo	HUMANA	NO APLICA	ALT	BAIXA
Indisponiblitat del personal	HUMANA	NO APLICA	MITJÀ	MITJA
Extorsió	HUMANA	ALTA	ALT	BAIXA
Enginyeria social	HUMANA	ALTA	ALT	MITJA

18.3 Tipus d'actius:

- **Usuaris:** totes aquelles persones que interactuen amb l'aplicació, aportant, modificant, o aprovant informació, així com els responsables del manteniment o del desenvolupament de noves funcionalitats o aplicacions.
- **Interfaces:** canals de comunicació d'informació de manera manual o automàtic amb altres aplicacions o organitzacions.
- **Software:** comprèn el programari necessari per al funcionament de l'aplicació.
- **Hardware:** engloba tots els elements físics (equipament informàtic) necessaris per al funcionament de l'aplicació.
- **Infraestructures:** són tots aquells actius relacionats amb l'entorn físic

- **Serveis:** serveis compartits, normalment, amb altres activitats de la companyia.
- **Dades i registres:** totes les dades de les bases de dades i els registres (logs) del sistema.
- **Documentació:** documentació, llicències i contractes que s'apliquen a les activitats que es desenvolupen dins de l'abast del sistema.

18.4 Actius

Actiu	Descripció	Responsable	Ubicació	Tipus actiu	Criticitat
CPD1	CPD CP	CIO	Edifici Casa de la Vila	Infraestructures	MOLT CRITIC
CPD2	CPD SG	CIO	Edifici Nau Sud	Infraestructures	CRITIC
Casa de la Vila	Oficines centrals	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
Recepció 1 CP	Recepció CP	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
Recepció 2 CP	Recepció CP	Responsable Infraestructures	Resort CP	Infraestructures	ALT
SPA	Fitness & SPA	Responsable Infraestructures	Resort CP	Infraestructures	ALT
Recepció 1 SG	Recepció SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Recepció Africà	Recepció SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Recepció Atenció Client SG	Recepció SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MITJÀ
Bar Restaurant SG	Bar Restaurant SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Victoria	restaurant Victoria, Fleca Victoria, Super Victoria	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Anfiteatre	Restaurant Tarraco, Super Anfi, Fleca Anfi	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
BackStage	Zona BackStage Anfitetre	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Bar Annex Anfiteatre	Bar Annnex Anfiteatre	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Tecnic SO SG	Cabina DJ Anfiteatre	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Bar Oasis	Bar Oasis	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Bar Baobab	Bar Baobab	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Bar Gulí	Bar Gulí	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Bar Poli	Bar Poli	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT

Forum	Bar Restaurant Forum	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
masia	Restaurant la Masia	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
Mercat	Mercat	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
Paraiso	Bar Paraiso	Responsable Infraestructures	Resort CP	Infraestructures	ALT
Coco Loco	Bar Coco Loco	Responsable Infraestructures	Resort CP	Infraestructures	ALT
Animal Kingdom	Bar Animal Kingdom	Responsable Infraestructures	Resort CP	Infraestructures	ALT
Super CP/ Fleca CP/ Souvenirs CP	Super CP/ Fleca CP/ Souvenirs CP	Responsable Infraestructures	Resort CP	Infraestructures	MOLT ALT
Ediifci Polivalent CP	Edifci Policalent CP	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Super SG	Super SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Souvenirs SG	Souvenirs SG	Responsable Infraestructures	Camping/Resort SG	Infraestructures	MOLT ALT
Boutique	Boutique	Responsable Infraestructures	Camping/Resort SG	Infraestructures	ALT
Oficines Futbol Salou	Oficines Futbol Salou	Responsable Infraestructures	Complex Esportiu	Infraestructures	MOLT ALT
Mini Estadi	Mini Estadi	Responsable Infraestructures	Complex Esportiu	Infraestructures	MOLT ALT
Serveis 1 CP	Serveis 1	Responsable Infraestructures	Resort CP	Infraestructures	ALT
Serveis 2 CP	Serveis 2	Responsable Infraestructures	Resort CP	Infraestructures	ALT
SAI CPD1	SAI que dona servei a CPD1	Responsable Infraestructures	CPD1	Infraestructures	MOLT CRITIC
SAI CPD2	SAI que dona servei a CPD2	Responsable Infraestructures	CPD2	Infraestructures	CRITIC
SAI Boutique	SAI que dona servei a Boutique	Responsable Infraestructures	Boutique	Infraestructures	MOLT ALT
SAI	SAI que dona servei a la restra de infrastructures	Responsable Infraestructures		Infraestructures	ALT
A/C CPD1	Aire Condicionat de CPD1	Responsable Infraestructures	CPD1	Infraestructures	MOLT CRITIC
A/C CPD2	Aire Condicionat de CPD2	Responsable Infraestructures	CPD2	Infraestructures	CRITIC
A/C Boutique	Aire Condicionat de Boutique	Responsable Infraestructures	Boutique	Infraestructures	MOLT ALT
Fibra Fosca	Aire Condicionat de Boutique	Responsable Infraestructures	Boutique	Infraestructures	MOLT CRITIC
SrvMilestone	Servidor Videovigilància	Tecnic1	CPD CP	Hardware	MOLT ALT
SrvTV-IP	Servidor TV-IP	Tecnic1	CPD SG	Hardware	MOLT ALT
SrvW2012[1]	Servidor DC físic	Tecnic1	CPD CP	Hardware	CRITIC
SrvW2012[2]	Servidor DC físic	Tecnic1	CPD SG	Hardware	CRITIC
Node Hypervisor[1]	Node HyperVisor 1	CIO	CPD CP	Hardware	CRITIC
Node Hypervisor[2]	Node HyperVisor 2	CIO	CPD SG	Hardware	CRITIC
Storage NetApp[1]	Controladora NetApp CPD1	CIO	CPD CP	Hardware	CRITIC
Storage NetApp[2]	Controladora NetApp CPD2	CIO	CPD SG	Hardware	CRITIC

Fortigate[1_1]	Firewall de CPD1	CIO	CPD CP	Hardware	CRITIC
Fortigate[1_2]	Firewall de CPD2	CIO	CPD SG	Hardware	CRITIC
HPE Aruba Servers[1]	Switch	CIO	CPD Primari	Hardware	CRITIC
HPE Aruba Servers[2]	Switch	CIO	CPD Primari	Hardware	CRITIC
Switch CORE[1_1]	Switch	CIO	CPD Primari	Hardware	MOLT CRITIC
Switch CORE[1_2]	Switch	CIO	CPD Primari	Hardware	CRITIC
Switch	Switch	Tecnic1	CPD Primari	Hardware	MOLT ALT
Router Root	Router	Tecnic1	CPD CP	Hardware	MOLT ALT
Router Backup	Router	Tecnic1	CPD CP	Hardware	ALT
AP	Acces Point Wifi	Tecnic1	CPD CP	Hardware	MITJÀ
UnitatCintes	Unitat de Cintes	Tecnic1	CPD CP	Hardware	MITJÀ
LTOs[1-5]	Cintes de backup LTO	Tecnic1	CP,SG	Hardware	MITJÀ
Smartphone[1-100]	Telefon smartphone de cada empleat	Tecnic1	CP,SG i FS	Hardware	MITJÀ
Portatil[1-4]	Portàtil de cada empleat	Tecnic1	casa de la Vila	Hardware	MITJÀ
Ordinador [1-200]	Portàtil de cada empleat	Tecnic1	CP,SG i FS	Hardware	MITJÀ
TPV[1-50]	Portàtil de cada empleat	Tecnic1	CP,SG i FS	Hardware	ALT
Impresora Laser	Impressora termica(TPVs i recepcions)	Tecnic1	CP,SG i FS	Hardware	ALT
Impresora Termica	Impresora Laser(Oficines i recepcions)	Tecnic1	CP,SG i FS	Hardware	ALT
Centraleta CPD CP	Centraleta telefònica CPD1	Tecnic1	CPD1	Hardware	MOLT ALT
Centraleta Boutique	Centraleta Telefònica Boutique	Tecnic1	Boutique	Hardware	MOLT ALT
VMachine[1-10]	Maquines Virtuals Critiques	Tecnic2	Nodes[1-2]	Software	MOLT CRITIC
Vmachine [11-20]	Maquines Virtuals	Tecnic2	Nodes[1-2]	Software	MOLT ALT
WebServer webs marketing	Host pagina web	Tecnic2	Hosting web	Software	MITJÀ
WebServer Reserves	Host pagina web	Tecnic2	Hosting web	Software	CRITIC
MailServer Office365	Servidor correu	Tecnic2	Hosting web	Software	MOLT ALT
MailServer Zimbra	Servidor correu	Tecnic2	Nodes[1-2]	Software	ALT
Smtp Zimbra	Servidor smtp	Tecnic2	Nodes[1-2]	Software	CRITIC
SQLServer	Base de dades(Navision,Salto, Labor)	Tecnic3	Nodes[1-2]	Dades i registres	CRITIC
MySQL Restauració [2]	Base de dades de restauració	Tecnic3	Nodes[1-2]	Dades i registres	MOLT ALT

HFSQL Reserves[2]	Base de dades de Reserves	Tecnic3	Nodes[1-2]	Dades i registres	CRITIC
File Server	Fitxers del servidor de fitxers	Tecnic3	Nodes[1-2]	Dades i registres	MOLT ALT
Dades als Discs	Dades als discs	Tecnic3	Nodes[1-2]	Dades i registres	MOLT ALT
Dades als Mòbils	Dades als mòbils	Tecnic3	Nodes[1-2]	Dades i registres	MOLT ALT
Dades als Emails Office365	Dades als discs	Tecnic3	Cloud	Dades i registres	MOLT ALT
Dades als Emails Zimbra	Dades als discs	Tecnic3	Nodes[1-2]	Dades i registres	MOLT ALT
Dades als WebServers Marketing	Dades als servers	Tecnic3	Cloud	Dades i registres	MOLT ALT
Dades als WebServers Reserves	Dades als servers	Tecnic3	Cloud	Dades i registres	MOLT CRITIC
Dades a Internet no controlades	Dades a Internet	Tecnic3	Cloud	Dades i registres	CRITIC
Win10License	Llicencia de Windows 10 de cada portàtil	Tecnic4	casa de la Vila	Documentació	BAIX
W2012License	Llicencia de windows server de cada servidor	Tecnic4	casa de la Vila	Documentació	BAIX
Office 365 License	Llicencia de Correu de Office 365	Tecnic4	casa de la Vila	Documentació	BAIX
OfficeLicense	Llicencia de Office	Tecnic4	casa de la Vila	Documentació	BAIX
Persona lIntern	Tot el personal intern.	RRHH	Personal	Usuaris	ALT
Direccio	Directors de la companyia	Direcció	Personal	Usuaris	MOLT ALT
Persona lSeguretat	Personal de seguretat extern	RRHH	Personal	Usuaris	MITJÀ

18.5 Amenaces

ID Amenaça	Amenaça	Origen	Motivació	IMPACTE	PROBABILITAT
A1	**Foc**	NATURALS	NO APLICA	ALT	BAIXA
A1	**Danys per aigua**	NATURALS	NO APLICA	ALT	BAIXA
A1	**Desastres naturals**	NATURALS	NO APLICA	ALT	MOLT BAIXA
B1	**Fuga d'informació**	HUMANA	ALTA	ALT	MITJA
B2	**Introducció de falsa informació**	HUMANA	ALTA	ALT	MITJA
B3	**Alteració de la informació**	ENTORN/ACCIDENTS	ALTA	ALT	MITJA
B4	**Corrupció de la informació**	ENTORN/ACCIDENTS	NO APLICA	ALT	ALTA

B5	**Destrucció de informació**	ENTORN/ACCIDENTS	MITJA	ALT	MITJA
B6	**Interceptació d'informació (escolta)**	HUMANA	MITJA	ALT	MITJA
B7	**Tallada del suministrament elèctric**	ENTORN/ACCIDENTS	MITJA	ALT	MITJA
B8	**Condicions inadecuades de temperatura o humitat**	ENTORN/ACCIDENTS	MITJA	ALT	ALTA
B9	**Fallada de serveis de comunicacions**	ENTORN/ACCIDENTS	NO APLICA	ALT	MITJA
B10	**Interrupció d'altres serveis i subministres esencials.**	ENTORN/ACCIDENTS	NO APLICA	MITJÀ	MITJA
B11	**Desastres industrials**	ENTORN/ACCIDENTS	NO APLICA	ALT	BAIXA
B12	**Malfuncionament dels equips**	ENTORN/ACCIDENTS	NO APLICA	ALT	MITJA
C1	**Degradación dels soporte d'emmmagatzament de la informació**	ENTORN/ACCIDENTS	NO APLICA	ALT	BAIXA
C2	**Difusió de malware**	HUMANA	ALTA	ALT	MITJA
C3	**Errors de manteniment / actualització de programas (software)**	HUMANA	NO APLICA	ALT	ALTA
C4	**Errors de manteniment / actualització d'equips (hardware)**	HUMANA	BAIXA	ALT	MITJA
C5	**Caiguda del sistema per sobrecarga**	HUMANA	NO APLICA	ALT	BAIXA
C6	**Pérdua d'equips**	HUMANA	NO APLICA	ALT	BAIXA
C7	**Indisponibilitat del personal**	HUMANA	NO APLICA	MITJÀ	MITJA
C8	**Abus de privilegis d'accés**	HUMANA	ALTA	ALT	MITJA
C9	**Acces no autoritzat**	HUMANA	ALTA	ALT	MITJA
D1	**Errors d'usuaris**	HUMANA	NO APLICA	MITJÀ	ALTA
D2	**Errors de l'administrador**	HUMANA	NO APLICA	ALT	MITJA
D3	**Errors de configuració**	HUMANA	NO APLICA	ALT	ALTA
E1	**Denegació de servei**	HUMANA	NO APLICA	ALT	BAIXA
E2	**Robo**	HUMANA	NO APLICA	ALT	BAIXA
E3	**Indisponibilitat del personal**	HUMANA	NO APLICA	MITJÀ	MITJA
E4	**Extorsió**	HUMANA	ALTA	ALT	BAIXA
E5	**Ingeniería social**	HUMANA	ALTA	ALT	MITJA

18.6 Creuament Actiu Amenaces.

ID	Amenaça	Usuaris	Interfaces	Software	Hardware	Infrastructures	Serveis	Dades i registres	Documentació
A1	**Foc**	Si	Si	Si	Si	Si	Si	Si	Si
A1	**Danys per aigua**	Si	Si	Si	Si	Si	Si	Si	Si
A1	**Desastres naturals**	Si	Si	Si	Si	Si	Si	Si	Si
B1	**Fuga d'informació**	No	Si	Si	No	No	Si	Si	Si
B2	**Introducció de falsa informació**	No	Si	Si	No	No	Si	Si	Si
B3	**Alteració de la informació**	No	Si	Si	No	No	Si	Si	Si
B4	**Corrupció de la informació**	No	Si	Si	No	No	Si	Si	Si

B5	**Destrucció de informació**	No	Si	Si	No	No	Si	Si	Si
B6	**Intercepció d'informació (escolta)**	No	Si	Si	No	No	Si	Si	Si
B7	**Tallada del subministrament elèctric**	No	Si	Si	Si	Si	Si	Si	Si
B8	**Condicions inadequades de temperatura o humitat**	No	Si	Si	Si	Si	Si	Si	Si
B9	**Fallada de serveis de comunicacions**	No	Si	Si	Si	Si	Si	Si	Si
B10	**Interrupció d'altres serveis i subministres essencials.**	No	Si	Si	Si	Si	Si	Si	Si
B11	**Desastres industrials**	No	Si	Si	Si	Si	Si	Si	Si
B12	**Malfuncionament dels equips**	No	Si	Si	Si	Si	Si	Si	Si
C1	**Degradació dels suports d'emmagatzemat de la informació**	No	Si	Si	Si	No	Si	Si	Si
C2	**Difusió de malware**	No	Si	Si	No	No	Si	Si	Si
C3	**Errors de manteniment / actualització de programes (software)**	No	Si	Si	No	No	Si	Si	Si
C4	**Errors de manteniment / actualització d'equips (hardware)**	No	Si	Si	Si	No	Si	Si	Si
C5	**Caiguda del sistema per sobrecarrega**	No	Si	Si	Si	No	Si	Si	Si
C6	**Pèrdua d'equips**	No	No	No	Si	No	No	Si	Si
C7	**Indisponiblitat del personal**	No	Si	Si	No	No	Si	Si	Si
C8	**Abús de privilegis d'accés**	No	Si	Si	Si	Si	Si	Si	Si
C9	**Accés no autoritzat**	No	Si	Si	Si	Si	Si	Si	Si
D1	**Errors d'usuaris**	No	No	Si	No	No	No	No	No
D2	**Errors de l'administrador**	No	Si	Si	Si	Si	Si	Si	Si
D3	**Errors de configuració**	No	Si	Si	No	No	Si	Si	Si
E1	**Denegació de servei**	No	Si	Si	No	Si	Si	Si	Si
E2	**Robo**	No	No	No	Si	Si	No	No	No
E3	**Indisponiblitat del personal**	Si	Si	Si	Si	Si	Si	Si	Si
E4	**Extorsió**	Si	Si	Si	Si	No	Si	Si	Si
E5	**Enginyeria social**	Si	Si	Si	Si	Si	Si	Si	Si

18.7 Valoració i càlcul del Risc.

18.7.1 Full de càlcul.

Per facilitar el càlcul del risc s'utilitza un full de càlcul que calcula el risc en base a la formula que he definida en la metodologia de riscos.

En la pestanya Risc veiem els resultats de l'anàlisi de riscos, utilitza les altres pestanyes per treure els valors.

S'ha calculat el risc tenint en compte el risc de cada amenaça multiplicat per la criticitat del actiu.

Amb aquest Excel només canviant els valors adequats es calcula el risc automàticament.

En aquesta fulla es mostra el valor obtingut de la formula i depenen d'aquest valor la cel·la pren un color o un altre.

Risc molt Alt El valor total és major o igual a 75, el color de la cel·la és vermell.

Risc Alt. El valor total es troba entre 45 i 74, el color de la cel·la és taronja.

.

Risc Mitjà. El valor total es troba entre 31 i 44 el color de la cel·la és groc.

Risc Baix. El valor total es troba entre 11 i 30 el color de la cel·la és blau.

Risc molt Baix. El valor total és menor o igual a 10 el color de la cel·la és verd.

Risc Null. El valor del risc es 0 el color de la cel·la és blanc.

Es pot determinar el risc total que suporta cada actiu, sumant el valor del Risc Ponderat de totes les amenaces que tenen relació sobre aquest actiu, aquest valor es por veure a la columna **Risc per Actiu.**

De la mateixa manera es pot calcular el valor del Risc per Amenaça, sumant el valor del Risc Ponderat de tots els actius relacionats amb aquesta amenaça, aquest valor es pot veure a la Fila **Risc per Amenaça.**

A partir d'aquesta informació ja es pot iniciar la fase de Gestió del Risc.

19 Amenaces i riscos detectats

19.1 Primer Anàlisi.

19.1.1 Taula de la suma dels riscs acumulats per amenaça:

Taula ordenada per risc acumulat.

	Amenaça	Risc acumulat
1.	Tallada del suministrament elèctric	6937,5
2.	Fallada de serveis de comunicacions	4625
3.	Condicions inadecuades de temperatura o humitat	3468,75
4.	Malfuncionament dels equips	3468,75

5.	Abus de privilegis d'accés	3468,75
6.	Acces no autoritzat	3468,75
7.	Errors de l'administrador	3468,75
8.	Foc	2381,25
9.	Danys per aigua	2381,25
10.	Interrupció d'altres serveis i subministres esencials.	2312,5
11.	Desastres industrials	1734,375
12.	Denegació de servei	1734,375
13.	Robo	1326,5625
14.	Corrupció de la informació	1223,4375
15.	Errors de manteniment / actualització de programas (software)	1223,4375
16.	Errors de configuració	1223,4375
17.	Errors de manteniment / actualització d'equips (hardware)	1087,5
18.	Errors d'usuaris	1087,5
19.	Desastres naturals	952,5
20.	Degradación dels soporte d'emmmagatzament de la informació	951,5625
21.	Caiguda del sistema per sobrecarga	951,5625
22.	Fuga d'informació	918,75
23.	Introducció de falsa informació	918,75
24.	Alteració de la informació	918,75
25.	Destrucció de informació	918,75
26.	Interceptació d'informació (escolta)	918,75
27.	Difusió de malware	815,625
28.	Pérdua d'equips	815,625
29.	Extorsió	137,5
30.	Ingeniería social	137,5
31.	Indisponibilitat del personal	0

Podem veure que les amenaces que representen un risc acumulat més gran són:

- Tallada del subministrament elèctric
- Fallada de serveis de comunicacions
- Condicions inadequades de temperatura o humitat
- Malfuncionament dels equips
- Abús de privilegis d'accés
- Accés no autoritzat
- Errors de l'administrador
- Foc
- Danys per aigua
- Interrupció d'altres serveis i subministres essencials.

19.1.2 Taula dels riscos acumulats per actiu:

Taula ordenada per risc acumulat per actiu.

	Actiu	Risc Acumulat Per Actiu
1.	SQLServer	1402,5
2.	MySQL Restauració[2]	1402,5
3.	HFSQL Reserves[2]	1402,5
4.	VMachine[1-10]	1374,375
5.	File Server	1168,75
6.	Dades als Discs	1168,75
7.	Dades als WebServers Reserves	1168,75
8.	Dades a Internet no controlades	1168,75
9.	WebServer Reserves	1145,3125
10.	Smtp Zimbra	1145,3125
11.	Dades als Mòbils	935
12.	Dades als Emails Office365	935
13.	Dades als Emails Zimbra	935
14.	Dades als WebServers Marketing	935
15.	VMachine[11-20]	916,25
16.	MailServer Office365	916,25
17.	Node Hypervisor[1]	821,25
18.	Node Hypervisor[2]	821,25
19.	Storage NetApp[1]	821,25
20.	Storage NetApp[2]	821,25
21.	Fortigate[1_1]	821,25
22.	Fortigate[1_2]	821,25
23.	HPE Aruba Servers[1]	821,25
24.	HPE Aruba Servers[2]	821,25
25.	Switch CORE[1_1]	821,25
26.	Switch CORE[1_2]	821,25
27.	MailServer Zimbra	687,1875
28.	SrvTV-IP	684,375
29.	Switch	684,375
30.	Router Root	684,375
31.	CPD1	680,625
32.	CPD2	680,625
33.	SAI CPD1	680,625
34.	SAI CPD2	680,625
35.	A/C CPD1	680,625
36.	A/C CPD2	680,625
37.	Fibra Fosca	680,625
38.	SrvMilestone	547,5
39.	SrvW2012[1]	547,5
40.	SrvW2012[2]	547,5
41.	Centraleta CPD CP	547,5

42.	Centraleta Boutique	547,5
43.	WebServer webs marketing	458,125
44.	Casa de la Vila	453,75
45.	Recepcio 1 CP	453,75
46.	Recepcio 2 CP	453,75
47.	Recepcio 1 SG	453,75
48.	Recepcio Africa	453,75
49.	Bar Restaurant SG	453,75
50.	Victoria(Restaurant,Super, Fleca)	453,75
51.	Anfiteatre	453,75
52.	BackStage	453,75
53.	Bar Annnex amfiteatre	453,75
54.	Tecnic SO SG	453,75
55.	Forum	453,75
56.	Restaurant La Masia	453,75
57.	Mercat	453,75
58.	Bar/Restaurant Paraiso	453,75
59.	Super CP/Fleca CP/ Souvenirs CP	453,75
60.	Super SG	453,75
61.	Souvenirs SG	453,75
62.	Boutique	453,75
63.	Oficines Futbol Salou	453,75
64.	Mini Estadi	453,75
65.	SAI Boutique	453,75
66.	Direccio	434,375
67.	PersonalIntern	347,5
68.	SPA	340,3125
69.	Bar Oasis	340,3125
70.	Bar Baobab	340,3125
71.	Bar Gulí	340,3125
72.	Bar Poli	340,3125
73.	Bar Coco Loco	340,3125
74.	Bar Animal Kingdom	340,3125
75.	Serveis 1 CP	340,3125
76.	Serveis 2 CP	340,3125
77.	SAI	340,3125
78.	A/C Boutique	340,3125
79.	Router Backup	273,75
80.	AP	273,75
81.	UnitatCintes	273,75
82.	LTOs[1-5]	273,75
83.	Smartphone[1-100]	273,75
84.	Portatil[1-4]	273,75
85.	Ordinador[1-200]	273,75

86.	TPV[1-50]	273,75
87.	Impresora Laser	273,75
88.	Impresora Termica	273,75
89.	Win10License	233,75
90.	W2012License	233,75
91.	Office 365 License	233,75
92.	OfficeLicense	233,75
93.	Recepcio Atenció Client SG	226,875
94.	Ediifci Policalent CP	226,875
95.	PersonalSeguretat	173,75

19.2 Infraestructures

19.2.1 CPD1

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	680,625

19.2.2 CPD2

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Accés no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos.	680,625

19.2.3 Casa de la Vila

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.4 Recepcio 1 CP

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.5 Recepcio 2 CP

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.6 SPA

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.7 Recepcio 1 SG

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.8 Recepcio Africa

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.9 Recepcio Atenció Client SG

No hi ha cap amenaça dintre dels rangs defiuna segona fase podríem tractar la seguent amenaça:

Amenaça	Valor
Tallada del suministrament elèctric	37,5

19.2.10 Bar Restaurant SG

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.11 Victoria(Restaurant,Super, Fleca)

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.12 Anfiteatre

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.13 BackStage

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.14 Bar Annnex Anfiteatre

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.15 Tecnic SO SG

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.16 Bar Oasis

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.17 Bar Baobab

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.18 Bar Gulí

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.19 Bar Poli

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.20 Forum

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.21 Restaurant La Masia

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.22 Mercat

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.2.23 Bar/Restaurant Paraiso

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.24 Bar Coco Loco

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.25 Bar Animal Kingdom

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.26 Super CP/Fleca CP/ Souvenirs CP

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.27 Ediifci Policalent CP

No hi ha cap amenaça dintre dels rangs definir segona fase podríem tractar la següent amenaça:

Amenaça	Valor
Tallada del suministrament elèctric	37,5

19.2.28 Super SG

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.29 Souvenirs SG

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.30 Boutique

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.31 Oficines Futbol Salou

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.32 Mini Estadi

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50
Suma de tots els riscos.	453,75

19.2.33 Serveis 1 CP

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.34 Serveis 2 CP

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.35 SAI CPD1

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.2.36 SAI CPD2

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.2.37 SAI Boutique

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.2.38 SAI

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.39 A/C CPD1

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25

Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.2.40 A/C CPD2

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.2.41 A/C Boutique

Amenaça	Valor
Tallada del suministrament elèctric	75

19.2.42 Fibra Fosca

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Fallada de serveis de comunicacions	75
Condicions inadequades de temperatura o humitat	56.25
Mal funcionament dels equips	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25

19.3 Hardware

19.3.1 SrvMilestone

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.3.2 SrvTV-IP

Amenaça	Valor
Tallada del suministrament elèctric	93.75
Condicions inadequades de temperatura o humitat	46.875
Fallada de serveis de comunicacions	62.5
Mal funcionament dels equips	46.875

Errors de manteniment / actualització d'equips (hardware)	46.875
Abús de privilegis d'accés	46.875
Acces no autoritzat	46.875
Errors de l'administrador	46.875
Suma de tots els riscos	684,375

19.3.3 SrvW2012[1]

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.3.4 SrvW2012[2]

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.3.5 Node Hypervisor[1]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.6 Node Hypervisor[2]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.7 Storage NetApp[1]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.8 Storage NetApp[2]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.9 Fortigate[1_1]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.10 Fortigate[1_2]

Amenaça	Valor
Tallada del suministrament elèctric	112,5

Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.11 HPE Aruba Servers[1]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.12 HPE Aruba Servers[2]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.13 Switch CORE[1_1]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25

Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.14 Switch CORE[1_2]

Amenaça	Valor
Tallada del suministrament elèctric	112,5
Condicions inadequades de temperatura o humitat	56.25
Fallada de serveis de comunicacions	75
Mal funcionament dels equips	56.25
Errors de manteniment / actualització d'equips (hardware)	56.25
Abús de privilegis d'accés	56.25
Acces no autoritzat	56.25
Errors de l'administrador	56.25
Suma de tots els riscos	821,25

19.3.15 Switch [261]

Amenaça	Valor
Tallada del suministrament elèctric	93.75
Condicions inadequades de temperatura o humitat	46.875
Fallada de serveis de comunicacions	62.5
Mal funcionament dels equips	46.875
Errors de manteniment / actualització d'equips (hardware)	46.875
Abús de privilegis d'accés	46.875
Acces no autoritzat	46.875
Errors de l'administrador	46.875
Suma de tots els riscos	684,375

19.3.16 Router Root

Amenaça	Valor
Tallada del suministrament elèctric	93.75
Condicions inadequades de temperatura o humitat	46.875
Fallada de serveis de comunicacions	62.5
Mal funcionament dels equips	46.875
Errors de manteniment / actualització d'equips (hardware)	46.875
Abús de privilegis d'accés	46.875
Acces no autoritzat	46.875

Errors de l'administrador	46.875
Suma de tots els riscos	684,375

19.3.17 Router Backup.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda.

19.3.18 AP

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic, l'organització ja disposa de Aps en repost per si deixés de funcionar algun d'ells.

19.3.19 Unitat Cintes

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda.

19.3.20 LTOs[1-5]

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda.

19.3.21 Smartphone[1-100]

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda, en específic, l'organització ja disposa de TPVs en repost per si deixés de funcionar algun d'ells.

19.3.22 Portàtil[1-4]

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda.

19.3.23 Ordinador[1-200]

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic, l'organització ja disposa de TPV en repost per si deixés de funcionar algun d'ells.

19.3.24 TPV[1-50]

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic, l'organització ja disposa de TPV en repost per si deixés de funcionar algun d'ells.

19.3.25 Impressora Làser

Amb l'anàlisi arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic, l'organització ja disposa de una impressora làser repost per si deixés de funcionar algun d'ells, també disposa d'un contracte de manteniment amb les empreses que li subministren les impressores laser.

19.3.26 Impressora Tèrmica

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic, l'organització ja disposa de varies en repost per si deixés de funcionar alguns d'elles.

19.3.27 Centraleta CPD CP

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.3.28 Centraleta Boutique

Amenaça	Valor
Tallada del suministrament elèctric	75
Fallada de serveis de comunicacions	50

19.4 Software

19.4.1 VMachine[1-10]

Amenaça	Valor
Fuga d'informació	56,25
Introducció de falsa informació	56,25
Alteració de la informació	56,25
Corrupció de la informació	84,375
Destrucció de informació	56,25
Interceptació d'informació (escolta)	56,25
Tallada del suministrament elèctric	112.5
Condicions inadecuades de temperatura o humitat	56,25
Fallada de serveis de comunicacions	75
Malfuncionament dels equips	56,25
Difusió de malware	56,25
Errors de manteniment / actualizació de programas (software)	84,275
Abus de privilegis d'accés	56,25
Acces no autoritzat	56,25
Errors d'usuaris	75
Errors de l'administrador	56,25
Errors de configuració	84.375
Suma dels Riscos	1374,375

19.4.2 VMachine[11-20]

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualizació de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	6,25

19.4.3 WebServer webs màrqueting

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.4.4 WebServer Reserves

Amenaça	Valor
Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	70,3125
Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	46,875
Condicions inadecuades de temperatura o humitat	70,3125
Fallada de serveis de comunicacions	46,875
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Errors de manteniment / actualització d'equips (hardware)	46,875
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125

19.4.5 MailServer Office365

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualització de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	56,25

19.4.6 MailServer Zimbra

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.4.7 Smtp Zimbra

Amenaça	Valor
Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	70,3125

Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	46,875
Condicions inadecuades de temperatura o humitat	70,3125
Fallada de serveis de comunicacions	46,875
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Errors de manteniment / actualització d'equips (hardware)	46,875
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125

19.5 Dades i registres

19.5.1 SQLServer

Amenaça	Valor
Fuga d'informació	56,25
Introducció de falsa informació	56,25
Alteració de la informació	56,25
Corrupció de la informació	84,375
Destrucció de informació	56,25
Interceptació d'informació (escolta)	56,25
Tallada del suministrament elèctric	112.5
Condicions inadecuades de temperatura o humitat	56,25
Fallada de serveis de comunicacions	75
Malfuncionament dels equips	56,25
Difusió de malware	56,25
Errors de manteniment / actualització de programas (software)	84,275
Abus de privilegis d'accés	56,25
Acces no autoritzat	56,25
Errors d'usuaris	75
Errors de l'administrador	56,25
Errors de configuració	84.375
Suma dels Riscos	1402,5

19.5.2 MySQL Restauració[2]

Amenaça	Valor
Fuga d'informació	56,25

Introducció de falsa informació	56,25
Alteració de la informació	56,25
Corrupció de la informació	84,375
Destrucció de informació	56,25
Interceptació d'informació (escolta)	56,25
Tallada del suministrament elèctric	112.5
Condicions inadecuades de temperatura o humitat	56,25
Fallada de serveis de comunicacions	75
Malfuncionament dels equips	56,25
Difusió de malware	56,25
Errors de manteniment / actualització de programas (software)	84,275
Abus de privilegis d'accés	56,25
Acces no autoritzat	56,25
Errors d'usuaris	75
Errors de l'administrador	56,25
Errors de configuració	84.375
Suma dels Riscos	1402,5

19.5.3 HFSQL Reserves[2]

Amenaça	Valor
Fuga d'informació	56,25
Introducció de falsa informació	56,25
Alteració de la informació	56,25
Corrupció de la informació	84,375
Destrucció de informació	56,25
Interceptació d'informació (escolta)	56,25
Tallada del suministrament elèctric	112.5
Condicions inadecuades de temperatura o humitat	56,25
Fallada de serveis de comunicacions	75
Malfuncionament dels equips	56,25
Difusió de malware	56,25
Errors de manteniment / actualització de programas (software)	84,275
Abus de privilegis d'accés	56,25
Acces no autoritzat	56,25
Errors d'usuaris	75
Errors de l'administrador	56,25
Errors de configuració	84.375
Suma dels Riscos	1402,5

19.5.4 File Server

Amenaça	Valor

Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	84,375
Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	93,75
Condicions inadecuades de temperatura o humitat	46,875
Fallada de serveis de comunicacions	62,5
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125
Suma dels Riscos	1168,75

19.5.5 Dades als Discs

Amenaça	Valor
Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	84,375
Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	93,75
Condicions inadecuades de temperatura o humitat	46,875
Fallada de serveis de comunicacions	62,5
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125
Suma dels Riscos	1168,75

19.5.6 Dades als Mòbils.

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualització de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	56,25

19.5.7 Dades als Emails Office365.

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualització de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	56,25

19.5.8 Dades als Emails Zimbra.

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualització de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	56,25

19.5.9 Dades als WebServers Marketing.

Amenaça	Valor
Corrupció de la informació	56,25
Condicions inadecuades de temperatura o humitat	56,25
Errors de manteniment / actualització de programas (software)	56,25
Errors d'usuaris	50
Errors de configuració	56,25

19.5.10 Dades als WebServers Reserves

Amenaça	Valor

Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	84,375
Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	93,75
Condicions inadecuades de temperatura o humitat	46,875
Fallada de serveis de comunicacions	62,5
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125
Suma dels Riscos	1168,75

19.5.11 Dades a Internet no controlades

Amenaça	Valor
Fuga d'informació	46,875
Introducció de falsa informació	46,875
Alteració de la informació	46,875
Corrupció de la informació	84,375
Destrucció de informació	46,875
Interceptació d'informació (escolta)	46,875
Tallada del suministrament elèctric	93,75
Condicions inadecuades de temperatura o humitat	46,875
Fallada de serveis de comunicacions	62,5
Malfuncionament dels equips	46,875
Difusió de malware	46,875
Errors de manteniment / actualització de programas (software)	70,3125
Abus de privilegis d'accés	46,875
Acces no autoritzat	46,875
Errors d'usuaris	62,5
Errors de l'administrador	46,875
Errors de configuració	70,3125
Suma dels Riscos	1168,75

19.6 Documentació.

19.6.1 Win10License.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.6.2 W2012License.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.6.3 Office 365 License.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.6.4 OfficeLicense.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.7 Usuaris

19.7.1 Personal Intern.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.7.2 Direcció.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.7.3 Personal Seguretat.

Amb l'anàlisi de l'annex 9.1 arribem a la conclusió que aquest actiu no necessita cap salvaguarda en específic.

19.8 Annex 10 - Proposta de projectes

20 Introducció.

Aquest document identifica projectes de seguretat de la informació i plans de tractament de riscos i les seves accions i plans de contingència per mitigar tots els riscos detectats en la fase d'identificació d'aquestes.

L'objectiu es crear un pla que permeti establir les mesures necessàries per garantir la continuïtat del negoci.

Els projectes proposats a continuació ajudaran a reduir el nivell de risc que en el punt anterior s'ha detectat com a risc potencial.

21 Implantació de polítiques de seguretat.

Un dels projectes més importants és la implantació de les polítiques de seguretat definides en l'Annex 2.

Per aconseguir aquest punt és molt important seguir un pla d'execució.

22 Pla de tractament del risc.

Per a aquells riscos que superin el nivell acceptable haurem de dur a terme un tractament. Aquest tractament pot portar a realitzar una de les següents accions:

Els controls de seguretat són fonamentals, ja que sense ells els riscos que estan per sobre del nivell acceptable suposaran un gran perill per al negoci i l'Organització.

El Pla de Tractament de Riscos conté una sèrie d'informació bàsica:

- Responsable del control: Persona que es responsabilitza de la correcta implantació del control
- Recursos: Persones, tècnics, empreses externes o materials que s'utilitzaran per a la implantació del control
- Accions a dur a terme: Accions que seran necessàries per a la implantació del control
- Prioritat: Tots els controls no tenen la mateixa prioritat, ja que d'una banda el nivell de risc no serà el mateix, ni tampoc el valor de cada actiu per l'Organització. Per tant cal establir prioritats. Aquesta prioritat pot venir determinada per la data d'implantació de cada control
- Pla d'execució.

A més a cada control hem associar-li una mètrica, que ens permetrà mesurar l'eficàcia del control. És a dir, les mètriques ens permetran saber si el control està funcionant adequadament o no.

Quan definim una mètrica, a més de la fórmula també és important definir els següents paràmetres:

- Responsable de la mètrica: Persona de l'Organització que s'encarregarà de gestionar el mesurament de l'indicador
- Valor límit: Valor de la mètrica a partir del qual podem considerar que el control no està funcionant del tot bé.
- Freqüència: Període que ha de transcórrer per mesurar. Habitualment els mesuraments tenen una periodicitat mensual, tot i que depèn molt del tipus de mètrica.

22.1 Accions

22.1.1 Eliminar el risc.

En alguns casos aplicant una salvaguarda o un control de seguretat podem eliminar el risc totalment.

En altres casos pot ser un actiu obsolet i el podem eliminar.

22.1.2 Reduir el risc a un nivell acceptable.

Aplicant controls de seguretat i salvaguardes fins reduir aquest risc a un nivell acceptable.

22.1.3 Assumir el risc.

En el cas de riscos que no siguin alts o molt alts es decideix assumir el risc.

22.1.4 Transferir el risc.

En cas de no tindre infraestructura adequada podem transferir el risc mitjançant terceres empreses que tinguin aquesta infraestructura o mitjançant assegurances.

23 Amenaces

23.1 Foc

Encara que no hi ha cap actiu afectat per aquesta amenaça, el risc acumulat col·loca aquest risc en el numero 8, per tant encara que inicialment podem pensar que no sigui quan mirem el risc acumulat es veu clarament que si que és una amenaça que té un risc alt.

L'organització compleix actualment la normativa vigent, per tant disposa d'extintors col·locats en totes les infraestructures i es segueix els controls que marca la normativa.

Actualment també un dels dos ressorts disposa de centraletes de control d'incendis centralitzades en un ordinador que envia alertes en cas d'incendis.

23.2 Danys per aigua

Encara que no hi ha cap actiu afectat per aquesta amenaça, el risc acumulat col·loca aquest risc en el numero 9, per tant encara que inicialment podem pensar que no sigui quan mirem el risc acumulat es veu clarament que si que és una amenaça que té un risc alt.

En aquest cas l'organització a decidit transferir aquest risc a tercers, i està cobert per les assegurances vigents.

23.3 Desastres naturals.

Cap actiu està afectat per aquesta amenaça, aquest risc està en la posició numero 19.

En aquest cas l'organització a decidit transferir aquest risc a tercers, i està cobert per les assegurances vigents.

23.4 Fuga d'informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 22, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'han de tractar.

23.4.1 Actius afectats.

23.4.1.1 Hardware

- SrvW2012[1]
- SrvW2012[2]
- Node Hypervisor[1]
- Node Hypervisor[2]
- Storage NetApp[1]
- Storage NetApp[2]
- Fortigate[1_1]
- Fortigate[1_2]
- HPE Aruba Servers[1]
- HPE Aruba Servers[2]
- Switch CORE[1_1]

- Switch CORE[1_2]

23.4.1.2 Software

- VMachine[1-10]
- WebServer Reserves
- Smtp Zimbra

23.4.1.3 Dades i registres

- SQLServer
- HFSQL Reserves[2]
- File Server
- Dades als Discs
- Dades als WebServers Reserves
- Dades a Internet no controlades

23.4.2 Salvaguardes.

Aquest risc el reduïm aplicant la política de seguretat definida en l'annex 2 i conscienciant i formant al personal.
S'han de definir i firmar acords de confidencialitat amb el personal directe i subcontractat i també a les empreses prestadores de serveis.
Aplicant una política de backup també definida a les polítiques de seguretat de l'annex 2.
Corregint altres amenaces també reduirem aquest risc com per exemple abús de privilegis d'accés, accés no autoritzat, etc...

23.5 Introducció de falsa informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 23, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.5.1 Actius afectats.

23.5.1.1 Hardware

- SrvW2012[1]
- SrvW2012[2]
- Node Hypervisor[1]
- Node Hypervisor[2]
- Storage NetApp[1]
- Storage NetApp[2]
- Fortigate[1_1]
- Fortigate[1_2]
- HPE Aruba Servers[1]
- HPE Aruba Servers[2]
- Switch CORE[1_1]
- Switch CORE[1_2]

23.5.1.2 Software

- VMachine[1-10]
- WebServer Reserves

- Smtp Zimbra

23.5.1.3 Dades i registres

- SQLServer
- HFSQL Reserves[2]
- File Server
- Dades als Discs
- Dades als WebServers Reserves
- Dades a Internet no controlades

23.5.2 Salvaguardes.

Aquest risc el reduïm aplicant la política de seguretat definida en l'annex 2 i aplicant una política de backup també definida a les polítiques de seguretat de l'annex 2.

23.5.2.1 Control de seguretat.

23.5.2.2 Mètrica.

23.6 Alteració de la informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 24, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.6.1 Actius afectats.

23.6.1.1 Hardware

- SrvW2012[1]
- SrvW2012[2]
- Node Hypervisor[1]
- Node Hypervisor[2]
- Storage NetApp[1]
- Storage NetApp[2]
- Fortigate[1_1]
- Fortigate[1_2]
- HPE Aruba Servers[1]
- HPE Aruba Servers[2]
- Switch CORE[1_1]
- Switch CORE[1_2]

23.6.1.2 Software

- VMachine[1-10]
- WebServer Reserves
- Smtp Zimbra

23.6.1.3 Dades i registres

- SQLServer
- HFSQL Reserves[2]
- File Server
- Dades als Discs

- Dades als WebServers Reserves
- Dades a Internet no controlades

23.6.2 Salvaguardes.

Aquest risc el reduïm aplicant la política de seguretat definida en l'annex 2 i aplicant una política de backup també definida a les polítiques de seguretat de l'annex 2.

23.6.2.1 Controls de seguretat.

Un control diari del funcionament de les copies de seguretat.

23.6.2.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 25% de copies fallides.

Freqüència: setmanal.

23.7 Corrupció de la informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 14, globalment és un risc que s'han de tractar i a més hi ha actius que tenen un risc que individualment s'ha de tractar.

23.7.1 Actius afectats.

23.7.1.1 Hardware

- SrvW2012[1]
- SrvW2012[2]
- Node Hypervisor[1]
- Node Hypervisor[2]
- Storage NetApp[1]
- Storage NetApp[2]
- Fortigate[1_1]
- Fortigate[1_2]
- HPE Aruba Servers[1]
- HPE Aruba Servers[2]
- Switch CORE[1_1]
- Switch CORE[1_2]

23.7.1.2 Software

- VMachine[1-10]
- WebServer Reserves
- Smtp Zimbra

23.7.1.3 Dades i registres

- SQLServer
- HFSQL Reserves[2]
- File Server

- Dades als Discs
- Dades als WebServers Reserves
- Dades a Internet no controlades

23.7.2 Salvaguardes.

Aquest risc el reduïm aplicant la política de seguretat definida en l'annex 2 i aplicant una política de backup també definida a les polítiques de seguretat de l'annex 2.

S'ha de fer una especial atenció als actius que estan allotjats al cloud.

23.7.2.1 Controls de seguretat.

Un control diari del funcionament de les copies de seguretat.

23.7.2.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 25% de copies fallides.

Freqüència: setmanal.

23.8 Destrucció de la informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 25, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.8.1 Salvaguardes.

Davant aquesta amenaça aplicarem tres tipus diferents de salvaguardes.

23.8.1.1 Backups.

A tots els actius allotjats en l'organització aplicant una política de copies de seguretat reduïm tots els riscos a un nivell acceptable per l'organització, aquesta política està definida a l'annex 2.

S'ha de fer una especial atenció als actius que estan allotjats al cloud.

23.8.1.2 Controls de seguretat.

Un control diari del funcionament de les copies de seguretat.

23.8.1.3 Mètrica.

- **Responsable mètrica:** tecnic1
- **Valor límit:** 25% de copies fallides.
- **Freqüència:** setmanal.

23.9 Intercepció d'informació (escolta)

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 14, globalment és un risc que s'han de tractar i a més hi ha actius que tenen un risc que individualment s'han de tractar.

23.9.1 Salvaguardes

Implementar controls, procediments i polítiques de transferència formals per protegir la transferència d'informació a través de les diferents alternatives de comunicació.

El detall dels controls, procediments i activitats ...

23.10 Tallada del subministrament elèctric.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 1, globalment és el risc més elevat, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

Com que és una amenaça amb un risc molt elevat, l'organització ja l'havia detectada i disposa de varis grups electrògens que garanteixen el subministrament elèctric propi per una durada de 12h, per garantir el subministrament elèctric en els talls mentrestant no salten el grups electrògens també s'han definit algunes salvaguardes.

23.10.1 Salvaguardes

- En tots els actius afectats per aquesta amenaça tindran que estar protegits per SAI(actualment és així en un 90% de les infraestructures, i en el 100% dels actius afectats).
- Tota d'instal·lació elèctrica que afecti aquesta actius haurà d'estar degudament documentada.
- En cada una les dos CPDs es posaran 2 SAIS per redundància.

23.10.1.1 Controls de seguretat.

Un control semestral del funcionament de SAIS.

23.10.1.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 0%.

Freqüència: semestral.

23.11 Condicions inadequades de temperatura o humitat

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 3, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.11.1 Salvaguardes

Reduïm aquesta amenaça col·locant sistemes de AA/CC i posant dispositius que ens controlin la temperatura i humitat i avisant-nos en cas que els valors surtin dels valors establerts.

Actualment totes les infraestructures critiques disposen de AA/CC.

És necessari posar un sistema de control de la temperatura i humitat en la CPD1, la CPD 2 ja disposa d'aquest element.

23.11.1.1 Controls de seguretat.

Un control diari del funcionament de sistemes de temperatura i humitat..

23.11.1.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 0%.

Freqüència: semestral.

23.12 Fallada de serveis de comunicacions.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 2, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.12.1 Salvaguardes

- Reduïm aquest risc
- Reduïm aquest risc posant en clúster els dispositius més importants.
- Reduïm aquest risc tenint dispositius en estoc de respost.
- Reduïm aquest risc posant sistemes de monitorització i emmagatzemant de logs, com ara nagios o ELK.
- Reduïm aquest risc amb contractes de manteniment a empreses de tercers.

23.12.1.1 Controls de seguretat.

Un control trimestral del funcionament de sistemes d'alta disponibilitat i de les unitats de respost.

23.12.1.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 0%.

Freqüència: trimestral

23.13 Interrupció d'altres serveis i subministres essencials.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 10, globalment és un del riscs que es col·loca en la zona mitjana.

23.13.1 Salvaguardes

- Reduïm aquest risc posant en clúster els dispositius més importants.
- Reduïm aquest risc tenint dispositius en estoc de repost.
- Reduïm aquest risc posant sistemes de monitorització i emmagatzemant de logs, com ara nagios o ELK.
- Reduïm aquest risc amb contractes de manteniment a empreses de tercers.

23.13.1.1 Controls de seguretat.

Un control trimestral del funcionament de sistemes d'alta disponibilitat i de les unitats de repost.

23.13.1.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 0%.

Freqüència: trimestral

23.14 Mal funcionament dels equips.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 4, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.14.1 Salvaguardes

- Reduïm aquest risc posant en clúster els dispositius més crítics afectats per aquesta amenaça.
- Reduïm aquest risc tenint dispositius en estoc de repost dels actius afectats.
- Reduïm aquest risc posant sistemes de monitorització i emmagatzemant de logs, com ara nagios o ELK.
- Reduïm aquest risc amb contractes de manteniment a empreses de tercers.

23.14.1.1 Controls de seguretat.

Un control trimestral del funcionament de sistemes d'alta disponibilitat i de les unitats de repost.

Un control semestral del nivell de resposta de les empreses externes dels contractes de manteniment acordats.

23.14.1.2 Mètrica.

Responsable mètrica: tecnic1

Valor límit: 0%.

Freqüència: trimestral en el cas de la comprovació dels sistemes d'alta disponibilitat i semestral amb el nivell de resposta de les empreses externes.

23.15 Degradació dels suport d'emmagatzemat de la informació.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 20, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.15.1 Salvaguardes

A tots els actius allotjats en l'organització aplicarem una política de copies de seguretat i així reduïm tots els riscos a un nivell acceptable per l'organització.

Tindre tots els sistemes crítics amb sistemes de RAID.

S'ha de fer una especial atenció als actius que estan allotjats al cloud.

23.15.1.1 Controls de seguretat.

Un control diari del funcionament de les copies de seguretat.

23.15.1.2 Mètrica.

- **Responsable mètrica:** tecnic1
- **Valor límit:** 25% de copies fallides.
- **Freqüència:** setmanal.

23.16 Difusió de malware.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 27, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.16.1 Salvaguardes

- Reduirem aquest risc tenint un sistema de antivirus a poder ser en tres capes, i en cada capa una AV diferent:
  - Av perimetral (fortinet)
  - AV de CORE (Kaspersky)
  - AV de equips (ESET)
- Formant i conscienciant al personal.
- Amb la política de seguretat definida a l'annex 2.
- Amb la política de Backups definida a l'annex 2.

23.17 Errors de manteniment / actualització de programes (software).

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 15, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.17.1 Salvaguardes

Reduïm aquest risc tenint entorns de test i proves i poder testar allí els manteniment i actualitzacions abans d'aplicar-ho en producció.

23.18 Errors de manteniment / actualització d'equips (hardware).

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 24, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.18.1 Salvaguardes

Reduïm aquest risc tenint entorns de test i proves i poder testar allí els manteniments i actualitzacions abans d'aplicar-ho en producció.

23.19 Pèrdua d'equips.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 28, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.19.1 Salvaguardes

- Aplicant les polítiques de seguretat definides a l'annex 2.
- Formant i conscienciant al personal.
- Assegurances
- Tenint els equips més crítics en repost.
- Tenint sistemes i aplicacions d'esborrat remot de dades.
- Encriptar els dispositius mòbils i dispositius com portàtils que surten a l'exterior.

23.20 Indisponiblitat del personal.

Cap actiu afectat per aquesta amenaça, i està col·locada en l'ultima posició.

L'organització decideix no tractar aquesta amenaça.

23.21 Abús de privilegis d'accés.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 5, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.21.1 Salvaguardes

- Monitoritzar accessos autoritzats, operacions privilegiades, intents d'accés no autoritzats els diferents sistemes i serveis. El monitoratge ha de realitzar-se de forma contínua. El detall dels controls, procediments i activitats.
- Controlar l'assignació de privilegis a usuaris dels diferents serveis, sistemes i sobretot bases de dades, mitjançant l'establiment d'un procediment formal que inclogui la respectiva autorització. El detall dels controls, procediments i activitats ...
- Mantenir un control sobre els drets d'accés dels usuaris als diferents programaris, serveis e infraestructures.

23.22 Accés no autoritzat.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 6, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.22.1 Salvaguardes

- Monitoritzar accessos autoritzats, operacions privilegiades, intents d'accés no autoritzats els diferents sistemes i serveis. El monitoratge ha de realitzar-se de forma contínua. El detall dels controls, procediments i activitats .
- Controlar l'assignació de privilegis a usuaris dels diferents serveis, sistemes i sobretot bases de dades, mitjançant l'establiment d'un procediment formal que inclogui la respectiva autorització. El detall dels controls, procediments i activitats ...

- Mantenir un control sobre els drets d'accés dels usuaris als diferents programaris, serveis e infraestructures.

23.23 Errors d'usuaris.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 18, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.23.1 Salvaguardes

- Registrar tota la informació possible dels esdeveniments generats per l'accés d' operadors als diferents sistemes i plataformes. Evitar l'ús de noms genèrics per a les identificacions de comptes d'usuaris.

23.24 Errors de l'administrador.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 7, globalment és un del riscs més elevats, queda més que clar que aquesta amenaça s'ha de tractar amb tots els esforços possibles per a reduir el nivell de risc.

23.24.1 Salvaguardes

- Monitoritzar canvis de configuració, sobre els diferents sistemes i serveis.
- Testejar els canvis en entorns de test abans de posar-los en producció.
- Registrar tota la informació possible dels esdeveniments generats per l'accés d'administradors als diferents sistemes i plataformes. Evitar l'ús de noms genèrics per a les identificacions de comptes d'usuaris.

23.25 Errors de configuració.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 16, globalment és un risc que s'han de tractar i a més hi ha actius que tenen un risc que individualment s'ha de tractar.

23.25.1 Salvaguardes

- Monitoritzar canvis de configuració, sobre els diferents sistemes i serveis.
- Testejar els canvis en entorns de test abans de posar-los en producció

23.26 Robatori.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 13, globalment és un risc que s'han de tractar i a més hi ha actius que tenen un risc que individualment s'ha de tractar.

23.26.1 Salvaguardes

23.27 Extorsió.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 29, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.27.1 Salvaguardes

- Reduïm l'amenaça a Extorsions aplicant directives de seguretat, formant i conscienciant al personal.

23.28 Enginyeria social.

Varis actius estan afectats per aquesta amenaça, i està col·locada en el numero 30, globalment no és un risc dels més elevats però si que hi ha actius que tenen un risc que individualment s'ha de tractar.

23.28.1 Salvaguardes

Reduïm l'amenaça a Extorsions aplicant directives de seguretat, formant i conscienciant al personal.

24 Risc residual.

En aquest apartat s'analitzarà el risc residual de cada amenaça de cada actiu després d'aplicar les salvaguardes.

Per la gran quantitat de actius (més de 3000 actius) aquest apartat queda fora de l'abast d'aquest TFM

25 Plans de contingència.

Es necessari tindre plans de contingències per garantir la continuïtat del negoci.

Per la gran quantitat de actius (més de 3000 actius) aquest apartat queda fora de l'abast d'aquest TFM.

25.1 Annex 11 – Auditoria

26 Objectiu de l'auditoria.

L'objectiu d'aquesta auditoria és mostrar el nivell de compliment de la norma ISO / IEC 27001 2005 sota el model de maduresa CMM i així veure reflectit el nivell d'implementació de la norma.

27 Abast auditoria.

L'abast d'aquesta primera auditoria està delimitada per la declaració d'aplicabilitat definida a l'annex 8.1.

28 Escala qualificació.

- Conformitat.
- Punt a millorar.
- No conformitat lleu.
- No conformitat greu.

29 Equip auditor.

- CIO.
- Responsable Seguretat.
- Tècnic 1 departament .
- Membre departament de qualitat.

30 Dates de l'execució auditoria.

- Inici auditoria: 11/05/19
- Fi Auditoria: 18/05/19

31 Informe executiu i conclusions

31.1 Nivell implementació.

Per a l'avaluació del grau de compliment es seguirà una notació de 0 a 5 de forma similar al Model de Maduresa, les equivalències són les següents:

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

La següent taula mostra el nivell d'implementació respecte la norma 27002

ISO 27002		
Control	**Descripció**	**Compliment**
A.5	Polítiques de seguretat.	DEFINIT
A.6	Organització de la seguretat de la Informació.	DEFINIT
A.7	Seguretat dels recursos humans.	DEFINIT
A.8	Gestió dels actius	GESTIONAT
A.9	Control d'accessos	GESTIONAT
A.10	Criptografia	INICIAL
A.11	Seguretat física i ambiental	GESTIONAT
A.12	Seguretat de les operacions	DEFINIT
A.13	Seguretat de les comunicacions	DEFINIT
A.14	Adquisició de sistemes, desenvolupament i	DEFINIT

	manteniment: requisits de seguretat dels sistemes d'informació.	
A.15	Relacions amb els Proveïdors..	DEFINIT
A.16	Gestió d'Incidències que afecten a la Seguretat de la Informació.	GESTIONAT
A.17	Continuïtat de seguretat de la informació	GESTIONAT
A.18	Compliment	GESTIONAT

31.2 Troballes

Control	Descripció	Qualificació
A.5	Polítiques de seguretat.	Conformitat
A.6	Organització de la seguretat de la Informació.	Punt a millorar
A.7	Seguretat dels recursos humans.	No conformitat lleu
A.8	Gestió dels actius	Punt a millorar
A.9	Control d'accessos	Punt a millorar
A.10	Criptografia	No conformitat greu
A.11	Seguretat física i ambiental	Punt a millorar
A.12	Seguretat de les operacions	No conformitat lleu
A.13	Seguretat de les comunicacions	No conformitat lleu
A.14	Adquisició de sistemes, desenvolupament i manteniment: requisits de seguretat dels sistemes d'informació.	No conformitat lleu
A.15	Relacions amb els Proveïdors..	No conformitat lleu
A.16	Gestió d'Incidències que afecten a la Seguretat de la Informació.	Punt a millorar
A.17	Continuïtat de seguretat de la informació	Punt a millorar
A.18	Compliment	Punt a millorar

31.3 Conclusions.

Si comparem el nivell d'implantació actual comparat amb el nivell inicial, es pot observar que s'ha millorat molt respecte a l'inici d'aquest pla director.

No obstant podem dir que encara que s'ha millorat molt encara dista molt d'estar ens uns nivells acceptables de seguretat.

Annex 12 – Conclusions i Anàlisi GAP Actual

32 Introducció

Amb el present anàlisi diferencial es pretén conèixer la distància entre la situació actual i el SGSI aplicat, tant del que s'especifica en la ISO / IEC 27001: 2005 com a la ISO / IEC 27002: 2005.

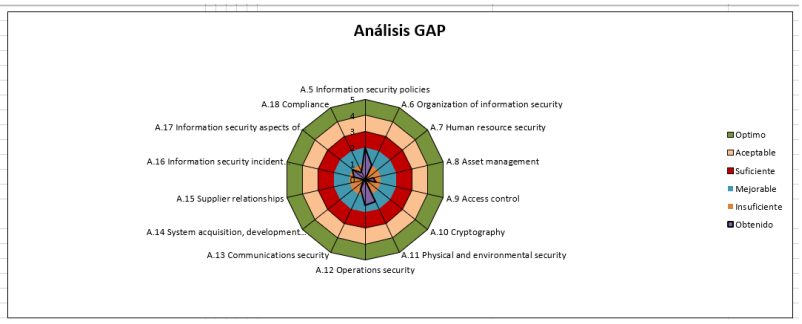
33 Notació.

Per a l'avaluació del grau de compliment es seguirà una notació de 0 a 5 de forma similar al Model de Maduresa, les equivalències són les següents:

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

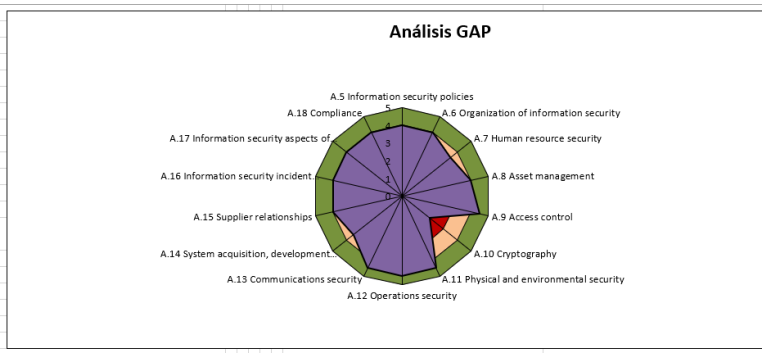
34 Estat Inicial

	Valor
A.5 Information security policies	2
A.6 Organization of information security	1
A.7 Human resource security	0
A.8 Asset management	0,5
A.9 Access control	0,73
A.10 Cryptography	0
A.11 Physical and environmental security	1,5
A.12 Operations security	1,6
A.13 Communications security	0,65
A.14 System acquisition, development and maintenance	0,2
A.15 Supplier relationships	0
A.16 Information security incident management	0,7
A.17 Information security aspects of business continuity management	1
A.18 Compliance	0,5



35 Estat Actual

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



36 Comparativa

CONTROL	INICIAL	ACTUAL	MILLORA
5. POLÍTIQUES DE SEGURETAT.	2	4	**2**
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.	1	4	**3**
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS.	0	3,5	**3,5**
8. GESTIÓ D'ACTIUS.	0,5	4	**3,5**
9. CONTROL D'ACCESSOS.	0,73	4,5	**3,8**
10. XIFRAT.	0	2	**2**
11. SEGURETAT FÍSICA I AMBIENTAL.	1,5	4,5	**3**
12. SEGURETAT A L'OPERATIVA.	1,6	4,5	**2,9**
13. SEGURETAT A LES TELECOMUNICACIONS.	0,65	4,5	**3,85**

14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.	0,2	4	**3,8**
15. RELACIONS AMB SUMINISTRADORES.	0	3,5	**3,5**
16. GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.	0,7	4	**3,3**
17. SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.	1	4	**3**
18. COMPLIMENT.	0,5	4	**3,5**