Pla Director de Seguretat de la Informació de Traun

Nom Estudiant: Maria Montserrat Ponce León

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

Àrea: Sistemes de Gestió de la Seguretat de la Informació

Consultor: Arsenio Tortajada Gallego

Professor responsable de l'assignatura: Carles Garrigues Olivella

Centre: Universitat Oberta de Catalunya

Data Lliurament: 06/06/2016

FITXA DEL TREBALL FINAL

Títol del treball:	*Pla Director de Seguretat de la Informació de Traun*
Nom de l'autor:	*Maria Montserrat Ponce León*
Nom del consultor/a:	*Arsenio Tortajada Gallego*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*06/2016*
Titulació o programa:	*Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)*
Àrea del Treball Final:	*Sistemes de Gestió de la Seguretat de la Informació*
Idioma del treball:	*Català*
Paraules clau	*Seguretat, anàlisi i amenaces*

Resum del Treball (màxim 250 paraules):

Aquest Treball de Fi de Màster pertany als estudis del Màster Interuniversitari de Seguretat de les Tecnologies de la Informació i Comunicació (MISTIC).

L'objectiu del projecte és l'elaboració d'un Pla Director de Seguretat per una farmacèutica-hospitalària, que s'anomenarà de manera fictícia Traun.

El Pla de Seguretat s'emmarca dins la norma ISO 27001:2013, i els codis de bones pràctiques esmentats en la ISO 27002:2013, que estableixen les especificacions per implementar, gestionar, supervisar i millorar un Sistema Gestor de Seguretat de la Informació (SGSI). S'ha realitzat un anàlisi de la situació actual de la seguretat en l'àmbit de les Tecnologies de la Informació i la Comunicació, per tal de poder definir uns objectius a curt i llarg termini i proposar un conjunt de projectes per tal d'arribar-hi. Dins d'aquest anàlisi realitzat podem destacar l'anàlisi diferencial, l'anàlisi de riscos (utilitzant MAGERIT com a metodologia) i l'anàlisi de compliment de la ISO.

Els progressos aconseguits en la implantació del SGSI són:

- Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la Norma i fixar l'abast i objectius.
- Establir una base documental i determinar les responsabilitats de cada un dels components de l'estructura organitzativa de seguretat, de manera que s'asseguri la realització de totes les tasques necessàries i proporcionar Revisió i Millora.

- Identificar i inventariar els actius crítics de l'Organització, determinar la magnitud de les amenaces i, en darrer terme, concretar els riscos als que estan exposats els diferents elements dels Sistemes d'Informació de l'Organització.
- A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la Seguretat de l'Organització.

Abstract (in English, 250 words or less):

This Final Master studies belong to the Master Interuniversity Security Information and Communication Technologies (MISTIC).

The objective of the project is the development of a Security Master Plan for a pharmaceutical-hospital, which fictitiously name is Traun.

The Security Plan is part of the ISO 27001: 2013 and the best practice set out in ISO 27002: 2013, establishing specifications to implement, manage, monitor and improve System Manager Information Security (ISMS). We made an analysis of the current state of security in the field of information and communications technology, in order to define short and long term objectives and propose a set of projects to reach -there. In this analysis we highlight the analysis conducted differential risk analysis (using methodology as MAGERIT) and analyzing compliance with ISO.

The progress achieved in the implementation of the ISMS are:

- Specify the status of the current information security in relation to different aspects of the standard and to establish the scope and objectives.
- Establish a documentary basis and determine the responsibilities of each of the components of the organizational structure of security, so as to ensure the completion of all necessary tasks and provide review and improvement.
- Identify and inventory the critical assets of the Organization, determine the magnitude of the threat, and ultimately realize the risks they are exposed to different elements of the information systems of the Organization.
- Based on the risks found, were selected and prioritized projects and a series of measures to improve the security of the Organization.

Índex

1. Introducció 8
1.1 Context i justificació del treball 8
1.2 Objectius del Treball 8
1.3 Enfocament i mètode seguit 8
1.4 Planificació del Treball 9
1.5 Breu sumari de productes obtinguts 10
1.6 Breu descripció dels altres capítols de la memòria 10
2. Contextualització 12
2.1. Descripció de l'empresa 12
2.2. Estructura organitzativa 12
2.3. Localització 12
2.4. IT Infraestructures 13
2.4.1. Sistemes 13
2.4.2. CPDs 14
2.4.3. Xarxes de comunicacions 14
2.4.4. Workstation i desktop 15
3. Objectius 16
4. Abast 16
5. Anàlisis diferencial 17
5.1. Anàlisis diferencial ISO/IEC 27002:2013 17
5.2. Resultats de Anàlisis diferencial ISO/IEC 27002:2013 20
6. Gestió Documental 21
6.1. Política de Seguretat 21
6.1.1. Introducció 21
6.1.2. Objectiu 21
6.2. Organització de la seguretat de la informació 21
6.3. Gestió de rols i responsabilitats 22
6.3.1. Comitè de direcció 22
6.3.2. Comitè de seguretat de la informació 22
6.3.3. Responsable de seguretat de la informació 23
6.3.4. Responsable de riscos 24
6.3.5. Resta d'àrees 25

6.4. Procediment d'auditories internes 25
6.5. Gestió d'indicadors de Seguretat 25
6.6. Procediment de revisió per direcció 27
6.7. Metodologia d'anàlisi de riscos 27
6.8. Declaració d'Aplicabilitat 28
7. Anàlisis de Riscos 33
7.1. Introducció 33
7.2. Inventari d'actius 33
7.3. Valoració dels actius 36
7.4. Dimensions de seguretat 37
7.5. Anàlisi d'amenaces 38
7.6. Impacte potencial 39
7.7. Nivell de Risc Acceptable i Risc Residual 44
7.8. Resultats 45
8. Propostes de Projectes 49
8.1. Introducció 49
8.2. Propostes 50
8.2.1. Projectes a curt termini 50
8.2.2. Projectes a mig termini 50
8.2.3. Projectes a llarg termini 50
8.3. Resultats 51
8.3.1. Evolució del risc 52
8.3.2. Evolució de la norma ISO/IEC 27002:2013 53
9. Auditoria de compliment 54
9.1. Introducció 54
9.2. Metodologia 54
9.3. Avaluació de la maduresa 55
9.4. Resultats 57
10. Conclusions 61
11. Glossari 62
12. Bibliografia 63
13. Annexos 64
ANNEX I- Anàlisis diferencial ISO/IEC 27002:2013 64

ANNEX II- Política de Seguretat 70
ANNEX III- Procediment d'auditoria interna 80
ANNEX IV- Procediment d'anàlisis i gestió de riscos 85
ANNEX V- Gestió d'indicadors de Seguretat 93
ANNEX VI- Declaració d'Aplicabilitat del SGSI 96
ANNEX VII- Inventari d'Actius i Risc Intrínsec 104
ANNEX VIII- Anàlisis d'amenaces 104
ANNEX IX- Anàlisis d'actius vs amenaces. 106
ANNEX X- Anàlisis d'actius vs Impacte Potencial 123
ANNEX XI- Projectes a curt termini 126
ANNEX XII- Projectes a mig termini 126
ANNEX XIII- Projectes a llarg termini 126
ANNEX XIV- Informe d'Auditoria 127

1. Introducció

1.1 Context i justificació del treball

Actualment, moltes organitzacions i empreses consideren la informació com un dels seus valors més importants. Això és així perquè la disponibilitat, integritat, confidencialitat i autenticitat d'aquesta informació, juntament amb els processos i elements que la tracten, són vitals i indispensables pel funcionament i supervivència d'aquestes empreses i organitzacions.

Degut al gran creixement que ha obtingut en aquest darrers anys l'organització Traun, recentment, s'ha creat un departament de Seguretat, per tal d'adaptar-se a les lleis de seguretat a nivell nacional e internacional i per millorar la seva seguretat de la informació desenvoluparem un Pla de Director de Seguretat.

1.2 Objectius del Treball

Els principals objectius són:

- Realitzar la Gestió de la Seguretat basada en un cicle de millora contínua.
- Preservar la Confidencialitat, Integritat i Disponibilitat de la informació.
- Compliment normatiu de la legislació vigent.
- Identificar els riscos més rellevants de l'organització.
- Implicar i conscienciar a tot el personal en la seguretat de la informació.

1.3 Enfocament i mètode seguit

La realització d'aquest projecte s'ha dividit en sis fases:

- Objectius del Pla director de seguretat i anàlisi diferencial respecte ISO/IEC 27001.
- Anàlisi de riscos.
- Proposta de projectes
- Auditoria del compliment
- Presentació dels resultats

En una primera fase, s'han definit els principals objectius del Pla director de Seguretat, s'ha determinat l'abast i s'ha realitzat un anàlisi diferencial on es valora la situació actual dels diferents punts de la ISO/IEC 27001 en Traun.
En la segona fase, s'han desenvolupat i generat els documents bàsics i algunes plantilles necessàries per l'adaptació a la norma ISO/IEC 27001.

En la tercera fase, s'han desenvolupat l'anàlisi de riscos dut a terme en la tercera fase ens aporta:

- Un anàlisi detallat dels actius més essencials relacionats amb la Seguretat de la Informació.
- Un estudi de les possibles amenaces a les que estan sotmesos els diferents actius analitzats.

- Una valoració de l'impacte potencial que suposaria per l'organització la materialització de les diferents amenaces a les que estan exposats els diferents actius analitzats.
- Una valoració del Risc Intrínsec per les diferents amenaces a les que estan exposats els diferents actius analitzats.
- El Risc Acceptable el qual esta disposat assumir l'organització.

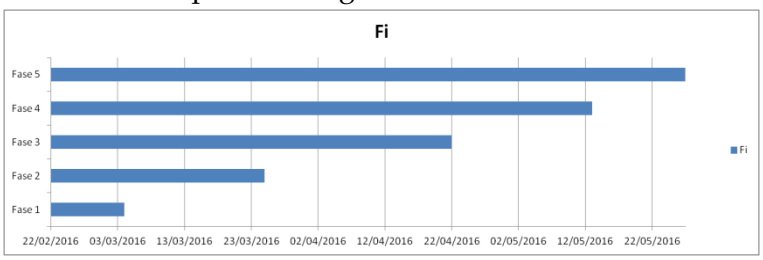
En la quarta fase, la proposta de projectes, s'han definit un cert nombre de projectes a realitzar els propers tres anys per tal de millorar certs aspectes relacionats amb la Seguretat de la Informació.

En la cinquena fase s'ha realitzat una auditoria de compliment de l'estàndard ISO/IEC 27002:2013.

En la sisena i última fase s'han realitzat els documents necessaris per tal de presentar els resultats i realitzar els informes requerits.

1.4 Planificació del Treball

Aquest projecte es desenvolupa en les següents fases:



- **Fase 1:** Situació actual: Contextualització, objectius i anàlisis diferencial

La 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.

- **Fase 2**: Sistema de Gestió Documental

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

- **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.

- **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.

- **Fase 5:** Auditoria de Compliment de la ISO/IEC 27002:2013

Avaluació de controls, maduresa i nivell de compliment.

1.5 Breu sumari de productes obtinguts

Els progressos aconseguits en la implantació del SGSI són:

- Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la Norma i fixar l'abast i objectius.
- Establir una base documental i determinar les responsabilitats de cada un dels components de l'estructura organitzativa de seguretat, de manera que s'asseguri la realització de totes les tasques necessàries i proporcionar Revisió i Millora.
- Identificar i inventariar els actius crítics de l'Organització, determinar la magnitud de les amenaces i, en darrer terme, concretar els riscos als que estan exposats els diferents elements dels Sistemes d'Informació de l'Organització.

A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la Seguretat de l'Organització

1.6 Breu descripció dels altres capítols de la memòria

Tal i com hem comentat en apartats anteriors, la memòria consta de 5 fases, entregades segons la planificació descrita anteriorment. A continuació realitzem un resum de les fases que veurem amb més detall en els pròxims apartats:

- **Fase 1:** Situació actual: Contextualització, objectius i anàlisis diferencial

S'estableix les bases d'un Pla director de seguretat per a l'empresa. Per simplificar, i com anirem veient, el nostre procés serà el següent:

  - Analitzar i detallar el nostre inventari d'actius.
  - Estudiar les amenaces a les que estem exposats.
  - Estudiar l'impacte potencial de les mencionades amenaces.
  - Proposar un pla d'acció per a lluitar contra aquestes amenaces.
  - Avaluar l'impacte residual un cop aplicat el pla d'acció.

- **Fase 2**: Sistema de Gestió Documental

La pròpia ISO/IEC 27001 defineix quins son els documents necessaris per a poder certificar el sistema, però per el desenvolupament del vostre treball us podeu centrar en els següents:

  - 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, us dels recursos de la Organització, comportament en cas d'incidents de seguretat, etc....
  - Procediment d'Auditories Internes: Document que ha d'incloure una planificació de les auditories que es portaran a terme durant la vigència del certificat (un cop s'obtingui), requisits que estabiran els auditors interns i es definirà el model d'informe d'auditoria.
  - Gestió d'Indicadors: Es necessari definir indicadors per a mesurar l'eficàcia dels controls de seguretat implantats. Igualment es important definir la sistemàtica per a fer les mesures.

- Procediment de Revisió per Direcció: La Direcció de l'Organització ha de revisar anualment les qüestions més importants que han anat passant en relació al Sistema de Gestió de Seguretat de la Informació. Per aquesta revisió, la ISO/IEC 27001 defineix, tant els punts d'entrada, com els punts de sortida que han d'obtenir-se.
- 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, es composa com a mínim d'una persona del comitè de direcció, d'aquesta manera les decisions que es prenguin podran estar aprovades prèviament per un membre de Direcció.
- Metodologia de Anàlisis de Riscos: Estableix la sistemàtica que s'haurà de seguir per a calcular el risc i ha d'incloure bàsicament la identificació i valoració dels actius, amenaces i vulnerabilitats.
- Declaració de Aplicabilitat: Document que inclou tots els controls de Seguretat establerts a la Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada.

L'existència de tots aquests documents constitueixen evidències de que el Sistema de Gestió està funcionant correctament.

- **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.

- **Fase 4:** Proposta de Projectes

La descripció de les millores proposades (projectes) hauran d'ajudar a mitigar el risc actual a l'Organització i evolucionar el compliment ISO fins al nivell adequat. Els mencionats projectes s'han de derivar dels resultats obtinguts del AARR, en base a les recomanacions associades a les amenaces identificades.

Els projectes plantejats seran resultants d'agrupar un conjunt de recomanacions identificades, a la fase d'anàlisi de riscos, per a facilitar la seva execució. S'incidirà, no només a la millora en la gestió de la seguretat, sinó també, en possibles beneficis col·laterals com poden ésser, la optimització de recursos, millora a la gestió de processos i tecnologies presents a l'organització analitzada.

- **Fase 5:** Auditoria de Compliment de la ISO/IEC 27002:2013

Arribats a aquesta fase, coneixem els actius de l'empresa i hem d'avaluar les amenaces. Es el moment de fer una parada al camí i avaluar fins a quin punt l'empresa compleix amb les "bones pràctiques" en matèria de seguretat. La ISO/IEC 27002:2013 ens servirà com a marc de control del estat de la seguretat.

2. Contextualització

En aquest projecte realitzarem un Pla Director de Seguretat per una farmacèutica-hospitalària, que s'anomenarà de manera fictícia Traun.

Degut al gran creixement que ha obtingut en aquest darrers anys, recentment, s'ha creat un departament de Seguretat, per tal d'adaptar-se a les lleis de seguretat a nivell nacional e internacional i per millorar la seva seguretat de la informació desenvoluparem un Pla de Director de Seguretat.

2.1. Descripció de l'empresa

L'empresa Traun disposa aproximadament 8.500 empleats dividits ens les 5 plantes industrials distribuïdes mundialment i 10 filials comercials.

Traun és un important productor mundial d'hemoderivats per al tractament de l'hemofília i altres dèficits congènits de factors de coagulació, malalties autoimmunes o deficiències congènites de la immunitat.

Per garantir la disponibilitat d'aquests tractaments, la seva qualitat i seguretat, Traun ha establert un sistema de producció global, des de l'obtenció del plasma a través d'una pròpia xarxa de centres de donació fins al producte acabat. Un sistema d'integració vertical que garanteix la seguretat i l'eficàcia dels seus medicaments.

2.2. Estructura organitzativa

A continuació detallem les diferents àrees/departaments:

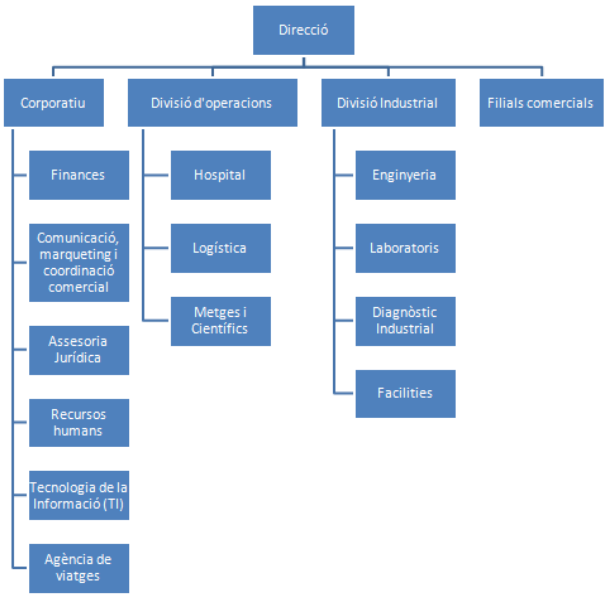
Direcció: President i equip directiu.

Corporatiu: Per a cada area existeix un màxim responsable que juntament amb els equips tècnics o administratius realitzen les seves pròpies tasques.

Divisió d'Operacions: En cada departament existeix un màxim responsable que juntament amb els seu equip realitzen l'extracció, anàlisis i repartiment del plasma.

Divisió Industrial: Per a cada area existeix un màxim responsable que juntament amb els seus equips realitzen els processos amb el plasma.

Filials comercials: Comercials i administratius que s'encarreguen de les funcions comercials en el seu país.

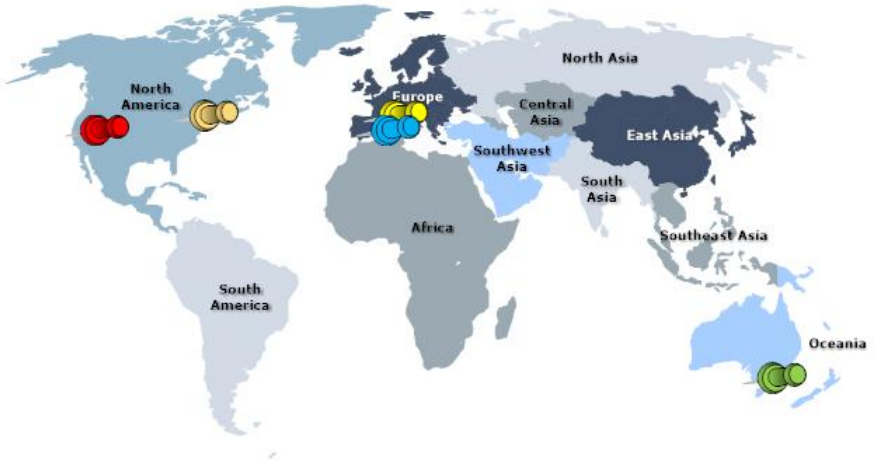


2.3. Localització

La seu corporativa central està situada a

Barcelona.
Les plantes industrials es troben a:

- Rubí, Barcelona
- Clayton, North Carolina, Estats Units
- Los Angeles, Califòrnia, Estats Units
- Melbourne, Austràlia



2.4. IT Infraestructures

Els elements relacionats amb les tecnologies de la Informació i la Comunicació existents es classifiquen en:

- Sistemes (servers)
- CPD
- Xarxes de comunicacions
- Workstation i desktop

2.4.1. Sistemes

Disposem de servidors tan virtuals com físics, amb les següents tecnologies a nivell de sistema operatiu:

- Red Hat 6.x
- Windows server 2012
- Windows 2008
- AIX 6.x
- Solaris 11.x

Aquests servers donen servei tan a les plantes de producció com a la part de sistemes, es a dir, alguns d'aquest sistemes son per donar suport a les plantes de producció amb les aplicacions necessàries (SCADA per exemple). I els servers que son per

l'administració, BBDD de donants, transaccions bancàries, pàgines web, BBDD de les formacions hospitalàries, viatges, etc.
A nivell d'aplicació per poder oferir tot ho esmentat anteriorment tenim:

- IIS
- Apache
- Tomcat
- Oracle database
- MySQL

2.4.2. CPDs

Disposem de 4 centres de processament de dades (CPD), ubicats en Rubi, Barcelona, North Carolina i Los Angeles.

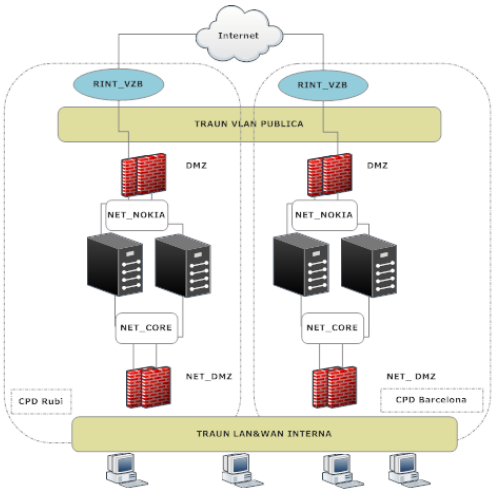
Els CPD son redundats, es a dir, Rubí té la contingència s Barcelona i North Carolina el té a Los Angeles. Donat que les dues principals fàbriques són idèntiques, els CPD també, per donar i abastir el mateix servei, tan a Carolina del Nord com a Rubi.

2.4.3. Xarxes de comunicacions

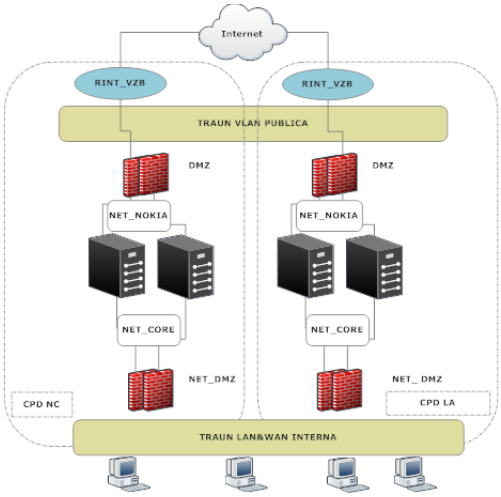
La xarxa de comunicacions són gestionades des dels servidors ubicats als diferents CPDs, segons la ubicació d'on es gestioni.

Observarem la similitud les diferents CPD, donat que han d'abastir el mateix servei de les plantes industrials i que entre ells estiguin redundats.

La xarxa de dades disposa de quatre tallafocs (redundats) i quatre xarxes, una anomenada externa, una de pública i dos zona DMZ. El diagrama de la xarxa de Catalunya es mostra a continuació:



El diagrama de xarxa dels CPDs D'Estats Units:



2.4.4. Workstation i desktop

Disposem d'una plantilla corporativa, Windows 7, que es desplega a totes el pc de sobretaula i portàtils. Durant l'any 2014 es va realitzar un projecte de migració i a dia d'avui tenim totes les estacions de treball amb la mateixa plantilla de windows 7. Possiblement durant aquest any s'iniciï un projecte per començar a migrar a Windows 10.

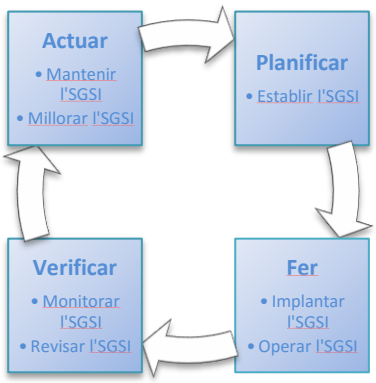
Cal destacar que els nostres usuaris de les estacions de treball es validen en l'Active Directory.

3. Objectius

Amb aquets Pla Director de Seguretat es pretén veure el estat actual de l'àrea IT de l'empresa, donat que des de direcció es va trobar amb la necessitat de tindre un departament de Seguretat, la primera part es veure en el estat que ens trobem.

Arrel d'aquest Pla, podrem evolucionar i millorar, veure las necessitat del negoci en quan quin es l'àrea que s'ha de millorar immediatament ,i els recursos necessaris per dur-la a terme.

Per la part de les àrees les quals ja es trobin implementades requerirà l'execució i revisió de certs controls de manera periòdica per tal de revisar que les mesures existents i les que es vagin executant al llarg del temps estiguin funcionant correctament. La metodologia del Pla que s'emprarà engloba tot el procés de millora contínua d'un sistema de gestió, és a dir, Planificar, Fer, Verificar i Actuar (PDCA, en les seves sigles en anglès).



En el nostre Pla seguirem les normes de la família ISO 27000, és a dir, les ISO/IEC 27001 i ISO/IEC 27002, publicades ambdues per la International Organization for Standardization (ISO).

4. Abast

L'abast d'aquest document és realitzar un Pla de director de Seguretat per a la part corporativa de l'empresa, on s'inclou tota la infraestructura de l'àrea IT, 'aquesta manera podem realitzar un pla de seguretat amb els elements vinculats a la Tecnologia de la Informació dedicada a donar servei a la resta d'àrees, on els nostres sistemes estan relacionats amb les transaccions bancàries, divisió industrial i dades confidencials dels donants.

En aquest document no abordarem la seguretat física dels edificis, ni els centres de donació, on possiblement interactuïn amb documentació confidencial sense cap tecnologia, i tampoc de les filials comercials.

5. Anàlisis diferencial

A continuació es detalla l'anàlisi diferencial de les mesures de seguretat i la normativa que té la Organització en relació a la Seguretat de la Informació. Aquest anàlisis diferencial es realitza respecte a als 114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius de control de la i ISO/IEC 27002, i ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

Aquesta valoració la realitzarem segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem.
10%	L1	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
50%	L2	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
90%	L3	Procés definit	La organització sencera participa al procés.
95%	L4	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
100%	L5	Optimitzat	Els processos estan sota constant millora.

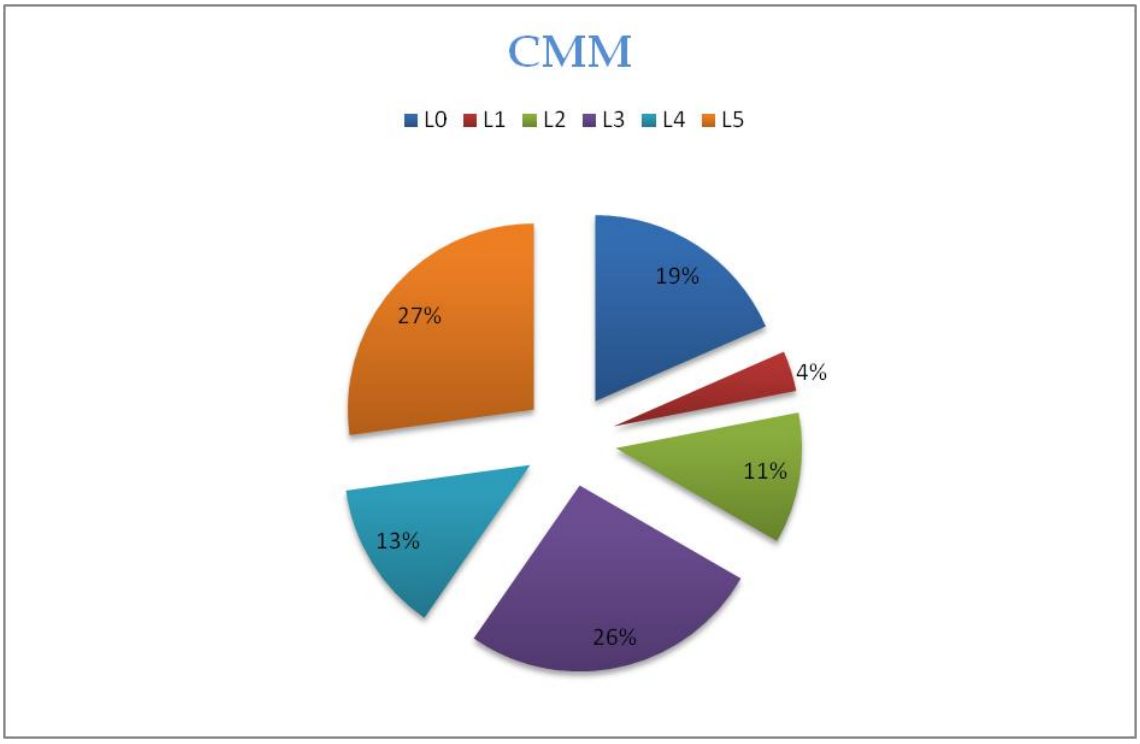
5.1. Anàlisis diferencial ISO/IEC 27002:2013

L'ANNEX I trobarem l'anàlisi diferencial amb més detall, CMM per als 114 controls i 35 objectius de control de la i ISO/IEC 27002.

A continuació veurem el resum de l'anàlisi diferencial segons els 14 àrees:

Controls	Situació Actual
5. Polítiques de la Seguretat de la Informació	L5
6. Organització de la Seguretat de la Informació	L3
7. La Seguretat dels recursos humans	L2
8. Gestió d'actius	L2
9. Control d'accés	L3
10 Criptografia	L0
11 La seguretat física i ambiental	L3
12 Operacions de Seguretat	L5
13 Seguretat de les comunicacions	L4
14 Sistema d'adquisició, desenvolupament i manteniment	L3

15 Les relacions amb proveïdors	**L4**
16 Gestió d'incidents de seguretat d'informació	**L0**
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	**L5**
18 Compliment	**L5**



Gràfica 1. Percentatge de controls segons valor CMM

Respecte als resultats anteriors comentarem els que es troben en pitjor estat i els que es troben més desenvolupats.

Controls	Situació Actual
5. Polítiques de la Seguretat de la Informació	**L5**
10. Criptografia	**L0**
12. Operacions de Seguretat	**L5**
16. Gestió d'incidents de seguretat d'informació	**L0**
17. Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	**L5**
18. Compliment	**L5**

Polítiques de la Seguretat de la Informació
Objectiu: Proporcionar orientació i suport per a seguretat de la informació, d'acord amb els requeriments del negoci i les lleis i reglaments pertinents de gestió.
Comentari: En aquest cas ens consta de que existeix la política de seguretat, tal i com es descriu a l'inici, l'àrea de seguretat es nova (any 2014), per tant encara no s'ha dut a terme cap revisió anual d'aquesta política, però existeix i a dia d'avui està implementada.

Criptografia
Objectiu: Per garantir l'ús adequat i eficaç de la criptografia per protegir la confidencialitat, autenticitat i / o integritat de la informació.
Comentari: No tenim cap document en referència a la criptografia ni intensió de dur a terme durant aquest any, una revisió de claus.

Operacions de Seguretat
Comentari: Aquest va ser el principal problema per a l'empresa, per aquest motiu es va integrar un departament de Seguretat, durant l'any 2015 s'han implementat i documentat gran part d'operacions i durant novembre 2015 la integració de la gestió de vulnerabilitats i gran part de compliment de polítiques, durant 2016 es farà revisions.

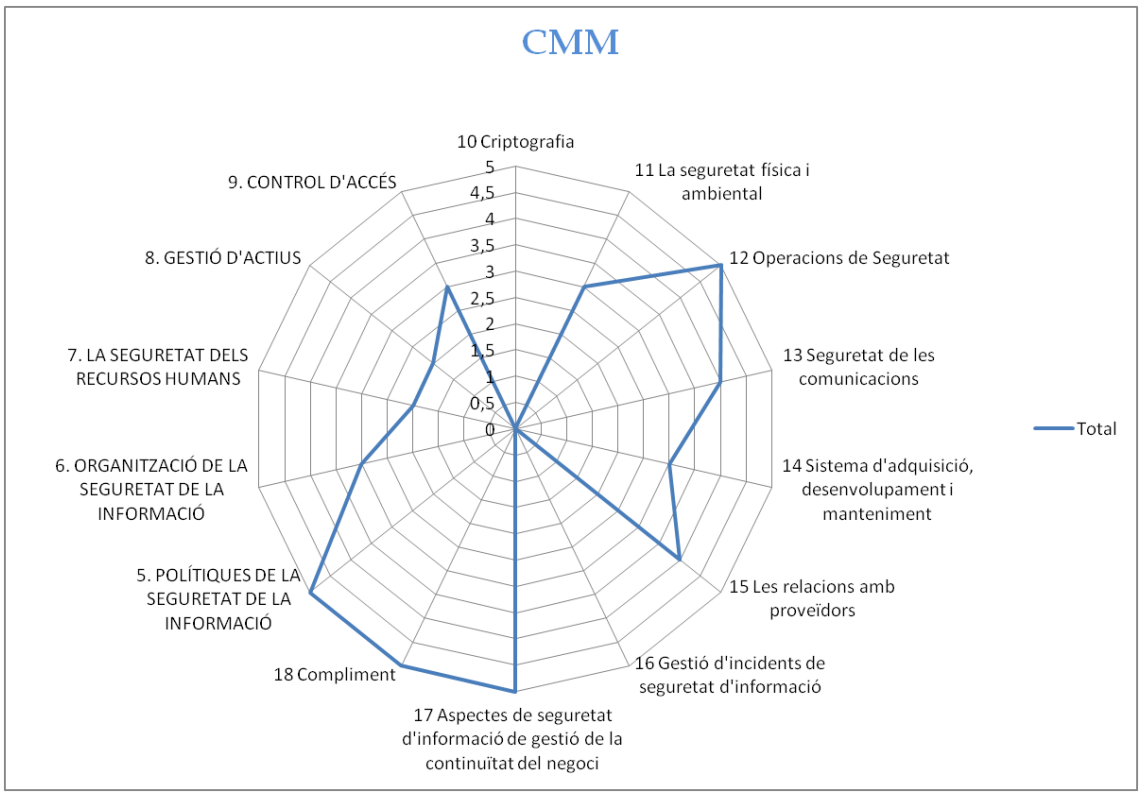
Gestió d'incidents de seguretat d'informació
Objectiu: Per garantir un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, incloent-hi la comunicació d'esdeveniments i debilitats de seguretat.
Comentari: Es va plantejar iniciar aquest control, però per la falta de recursos s'ha arribat a l'acord que ho portarà una empresa externa, la qual encara no esta contractada, per això aquest control es un L0.

Aspectes de seguretat d'informació de gestió de la continuïtat del negoci
Comentari: Aquests controls es troben més regulats, més per les àrees tècniques de TI que no pas per seguretat, ja que es un requeriment del negoci,el poder donar servei als donants i creant fàrmacs.

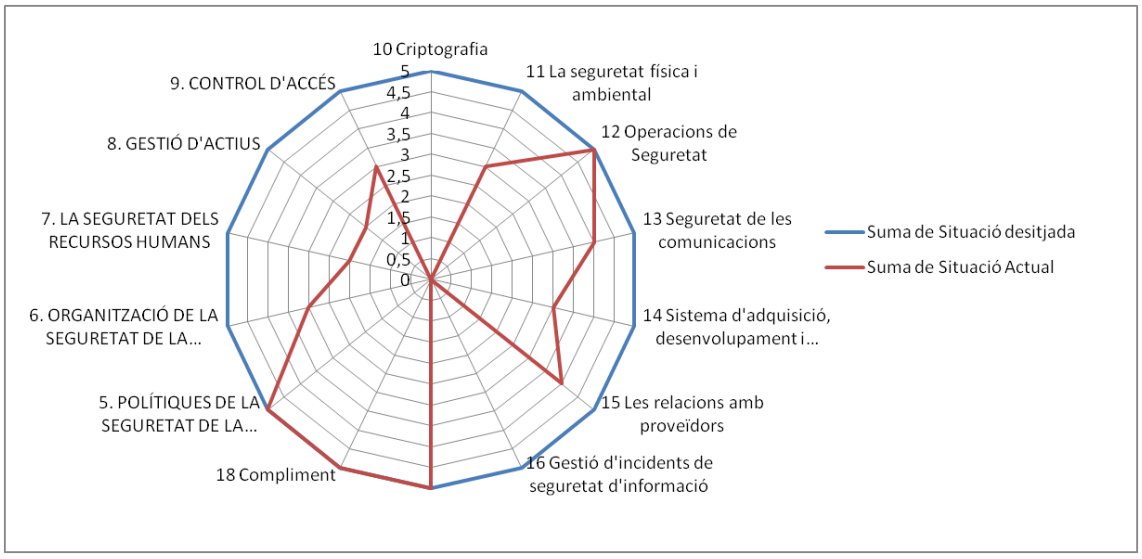
Compliment
Comentari: Per la part operacional s'ha mencionat que durant el final d'any ja es fan revisions tècniques de compliment, i a més a més, des de l'arrea de seguretat al gener s'ha contractat una empresa externa perquè ens revisi els controls, les polítiques, normes i procediments.

5.2. Resultats de Anàlisis diferencial ISO/IEC 27002:2013

En la gràfica següent podem observar el resultat de l'anàlisi diferencial, en general, donat que es tracta d'un nou departament en una gran empresa, encara ens trobem en una fase molt inicial on queda per definir objectius, i els controls es torben en un estat definició.



Gràfica 2. Estat de les àrees



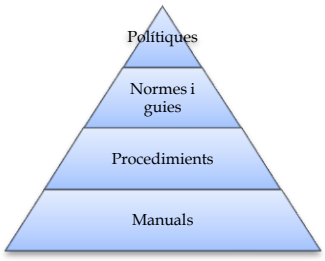
Gràfica 3. Estat de les àrees vs estat desitjat

6. Gestió Documental

6.1. Política de Seguretat

6.1.1. Introducció

L'estàndard per excel·lència en un sistema de gestió de la seguretat és, sens dubte, la política de seguretat de la informació, ja que constitueix el primer nivell de la piràmide jeràrquica en seguretat de la informació.



Podeu trobar el document de la política de seguretat en l'ANNEX II.

6.1.2. Objectiu

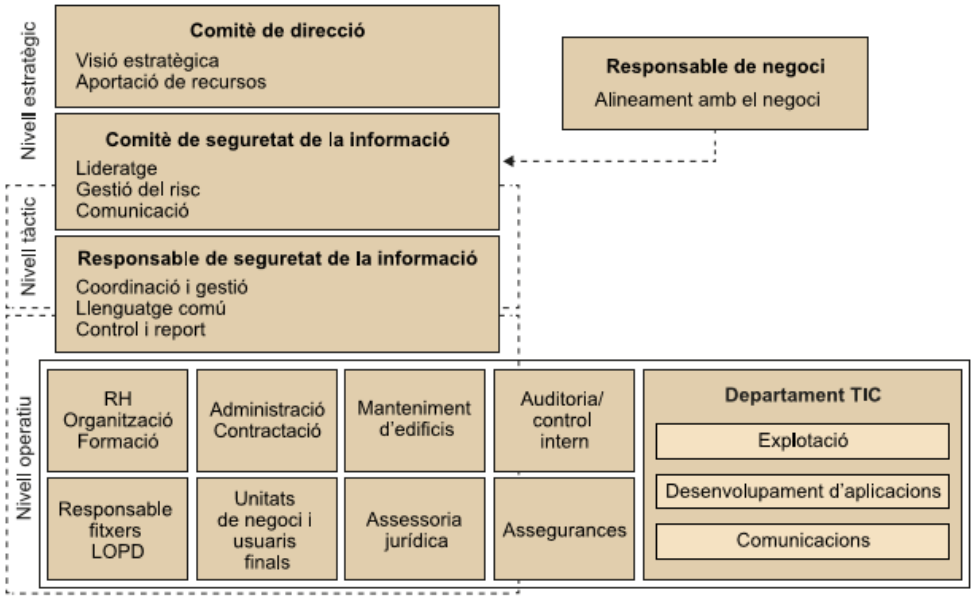
L'objectiu d'aquesta política és establir les directrius en seguretat de la informació, alineades amb els objectius del negoci i la legislació aplicable, i tot plegat confirmat i amb el compromís de la direcció de la companyia.

L'ISO 27002, a l'apartat 5, fa una descripció detallada de quin ha de ser el contingut de la política de seguretat de la informació i dels principals aspectes de la revisió d'aquesta política.

6.2. Organització de la seguretat de la informació

Estructura interna amb responsabilitat directa sobre la seguretat de la informació. A continuació s'exposa l'estructura organitzativa de seguretat de la informació la qual està formada per tres nivells:

- Nivell estratègic: On es determinen els objectius que es proposa.
- Nivell executiu: Punt de coordinació entre les diferents àrees per aconseguir els objectius.
- Nivell operatiu: on cada componen realitza la seva activitat.



Imatge 1. Estructura organitzativa (Ref: pàgina 29 mòdul 4 de SGSI)

6.3. Gestió de rols i responsabilitats

6.3.1. Comitè de direcció

Les funcions en matèria de seguretat de la informació del comitè de direcció de la companyia són les següents:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres d'un comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar riscos possibles introduïts per canvis en les funcions o en el funcionament de la companyia per a adoptar les mesures de seguretat més adequades.
- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en la matèria.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

Les decisions preses pel comitè de direcció en matèria de seguretat de la informació han de quedar recollides en acta.

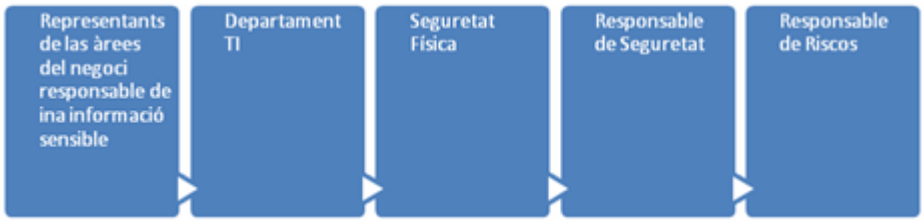
6.3.2. Comitè de seguretat de la informació

Les decisions en matèria de seguretat de la informació les pren de manera consensuada un grup format per diferents responsables dins de la companyia.

Les funcions en matèria de seguretat de la informació del comitè de seguretat de la informació són les següents:

- Implantar les directrius del comitè de direcció.
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.
- Validar el mapa de riscos i les accions de mitigació que ha proposat el responsable de seguretat de la informació.
- Validar el pla de seguretat de la informació o pla director de seguretat de la informació i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.
- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.
- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.
- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.
- Revisar les incidències més destacades.
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució de l'SGSI.

El comitè de seguretat de la informació té representació de diverses àrees de suport i també de les principals unitats de negoci (les que estan sotmeses a més riscos).



Imatge 2. Composició del comitè de seguretat a Traun.

6.3.3. Responsable de seguretat de la informació

La designació d'un responsable de seguretat de la informació (RSI) és l'única via per a avançar de manera organitzada i gradual en seguretat de la informació, ja que garanteix que hi ha algú per a qui la seguretat de la informació és una prioritat.

Les funcions en matèria de seguretat de la informació dels RSI són coordinar les accions orientades a garantir la seguretat de la informació en qualsevol de les formes que té (digital, òptica, paper, etc.) i en tot el cicle de vida d'aquesta informació (creació, manteniment, distribució, emmagatzematge i destrucció), per a protegir-la en termes de confidencialitat, privadesa, integritat, disponibilitat, autenticitat i traçabilitat.

Tot plegat es concreta en els punts següents:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius en matèria de seguretat de la informació.
- Desenvolupar i mantenir el document d'Organització de la seguretat de la informació en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les responsabilitats en seguretat i també una descripció detallada de funcions i dependències.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.
- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.
- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

6.3.4. Responsable de riscos

- Vetllar pel compliment legal (LOPD, RD 3/2010, Esquema nacional de seguretat, Basilea, SOX, etc.) i coordinar les actuacions necessàries amb les unitats responsables.
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.

- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).

6.3.5. Resta d'àrees

Cada àrea dins de la companyia ha de col·laborar amb l'RSI a desplegar la seguretat en el seu àmbit d'actuació i a aconseguir treballar i fer treballar l'organització de manera segura. Així, doncs, també s'han d'identificar funcions de seguretat en els àmbits d'auditoria, assegurances, formació, organització, etc.

6.4. Procediment d'auditories internes

La metodologia del Pla que s'emprarà engloba tot el procés de millora contínua d'un sistema de gestió, és a dir, Planificar, Fer, Verificar i Actuar (PDCA). Tal i com indica el cicle Deming hi ha d'haver-hi la fase de verificar.

Traun realitzarà anualment auditories per verificar que els controls, processos i procediments del Sistema de Gestió de Seguretat de la Informació segueix conforme la norma i la legislació vigent, així com validar que els objectius de seguretat de l'organització estan implementats, mantinguts amb eficàcia i tenen el rendiment esperat. En l'ANNEX III podem trobar el procediment d'auditories internes de Traun.

6.5. Gestió d'indicadors de Seguretat

Els indicadors de Seguretat són una manera de mesurar l'estat de Seguretat de la informació implantades en l'organització, també s'encarrega de mesurar l'eficàcia i l'eficiència. Tot indicador consta de vuit components bàsics:

1) Nom de l'indicador. S'ha de seleccionar un nom significatiu, no massa llarg, que doni idea de quin és el mesurament que es fa.
2) Descripció de l'indicador. Explicació de l'objectiu de mesura d'aquest indicador.
3) Control de seguretat a què dóna suport. A quin control o controls dóna cobertura.
4) Fórmula de mesurament. Descripció de la fórmula aplicada per a obtenir la mesura. És important que els paràmetres que hi intervenen siguin concrets i no es prestin a ambigüitat.
5) Unitats de mesura. Les unitats de mesura han d'estar especificades clarament.

6) Freqüència de mesura. Cada quant s'ha de recollir la mesura. És possible establir una freqüència inicial durant un període, i una freqüència posterior més gran (per exemple, quinzenal els tres primers mesos, i mensual a partir del quart mes). En qualsevol cas, la freqüència depèn de la variabilitat en el temps de la mesura.
7) Quan sigui possible, valor objectiu i valor llindar, és a dir, respectivament, quin és el valor correcte per a la companyia i quin és el valor per sota del qual s'ha d'aixecar una alarma.
8) Responsable de la mesura. Sobre qui o, preferiblement, sobre quin càrrec recau la responsabilitat de proporcionar el resultat de la mesura.

Hi ha diferents tipus d'indicadors (Ref: Mòdul 3 SGSI, pàg. 43).

- **Indicadors de gestió**
  - Nombre d'hores de formació impartides.
  - Pressupost dedicat a personal de manteniment de sistemes.
  - Nombre de treballadors amb responsabilitats en seguretat de la informació.
  - Nombre de suggeriments de millora de l'SGSI rebuts dels treballadors.

- **Indicadors d'operació**
  - Temps total de caiguda d'un determinat servei en l'últim mes.
  - Nombre d'avaries d'equips informàtics en l'últim mes.
  - Trànsit mitjà del tallafoc.
  - Nombre d'intents de penetració detectats per l'IDS respecte del nombre d'intents rebutjats.
  - Nombre de virus detectats respecte del nombre d'incidències per virus.

- **Indicadors d'entorn**
  - Alertes per un virus nou.
  - Temps mitjà d'exposició d'un sistema des que es detecta una vulnerabilitat fins que s'aplica el pegat.
  - Alertes meteorològiques per onades de calor, tempestes elèctriques, inundacions...
  - Canvis en la legislació.

A continuació es detallen els indicadors de Seguretat ja implementats en Traun, per veure amb més detall cada un dels indicadors implementats, consultar l'ANNEX V:

Controls	Indicador definit	En Procès	No Existeix
5. Polítiques de la Seguretat de la Informació	X		
6. Organització de la Seguretat de la Informació	X		
7. La Seguretat dels recursos humans		X	
8. Gestió d'actius			X
9. Control d'accés	X		
10 Criptografia			X

11 La seguretat física i ambiental			X
12 Operacions de Seguretat		X	
13 Seguretat de les comunicacions		X	
14 Sistema d'adquisició, desenvolupament i manteniment			X
15 Les relacions amb proveïdors		X	
16 Gestió d'incidents de seguretat d'informació			X
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci		X	
18 Compliment	X		

Hi ha diferents controls de la ISO encara no s'han desenvolupat ni definit un indicador, disposem d'un indicador per mesurar la implementació d'aquests:

PERCENTATGE D'IMPLEMENTACIÓ DE CONTROLS	
Objectiu de l'indicador	**Definició**
Busca identificar el grau d'avanç en la implementació de controls de seguretat	Grau d'avanç en la implementació de controls de seguretat.
Responsable de la mesura	**Freqüència**
Responsable de Seguretat	Mensual
Fórmula de mesurament	**Descripció dels valors**
IMCONT01=(CI/CN)*1000	CI: Nombre de controls Implementats CN: Nombre de controls que es planegen implementar
Valor objectiu de l'indicador	
75%	

6.6. Procediment de revisió per direcció

Tal i com està definit en Traun, tota la documentació d'alt nivell té definit una revisió periòdica per part de direcció.
Aquesta revisió del Sistema Gestor de Seguretat de la Informació es obligada com a mínim un cop l'any, i te com a objectiu assegurar que es adequat i efectiu pels propòsits i context de l'organització.

6.7. Metodologia d'anàlisi de riscos

L'anàlisi i gestió de riscos en tecnologies de la informació i la comunicació permet a qualsevol organització, sigui pública o privada, prendre decisions de gestió i assignar recursos amb perspectives i objectius concrets, ja siguin tecnològics, humans o financers.

El mètode Magerit, el que utilitzarem, ens aporta una metodologia per poder analitzar i gestionar els diferents riscos existents en qualsevol tipus d'organitzacions

L'ANNEX IV trobarem el procediment que té com a objectiu establir les activitats i responsabilitats necessàries per a la realització i posteriorment la gestió de riscos.

6.8. Declaració d'Aplicabilitat

La declaració d'aplicabilitat consisteix en definir com s'implementarà gran part del sistema de seguretat de la informació. L'objectiu principal és especificar quin dels 114 controls o mesures preventives són els que s'implementarà en l'organització. Per tant serà el document de referència per a una auditoria de certificació on es comproven els controls implementats.

A continuació es detalla els controls de la ISO/IEC 27002:2013 que son aplicables al SGSI, per veure el document de declaració d'aplicabilitat, consultar l'ANNEX VI:

Controls	Aplicabilitat
5. Polítiques de la Seguretat de la Informació	
5.1 Direcció de gestió de seguretat de la informació	
5.1.1 Les polítiques de seguretat de la informació	Aplica
5.1.2 Revisió de les polítiques de seguretat de la informació	Aplica
6. Organització de la Seguretat de la Informació	
6.1 Organització interna	
6.1.1 Rols i responsabilitats de seguretat de la informació	Aplica
6.1.2 La segregació de funcions	Aplica
6.1.3 Contacte amb les autoritats	Aplica
6.1.4 Contacte amb els grups d'interès especial	Aplica
6.1.5 Seguretat de la informació en la gestió de projectes	Aplica
6.2 Els dispositius mòbils i el teletreball	
6.2.1 política de dispositiu mòbil Una política de control	Aplica
6.2.2 El teletreball	Aplica
7. La Seguretat dels Recursos Humans	
7.1 Amb anterioritat a l'ocupació	
7.1.1 Control de Screening	Aplica
7.1.2 Termes i condicions d'ocupació	Aplica
7.2 Durant l'ocupació	
7.2.1 Les responsabilitats de gestió	Aplica
7.2.2 Conscienciació sobre la seguretat de la informació, l'educació i la formació	Aplica
7.2.3 Procés disciplinari	Aplica
7.3 Terminació i canvi d'ocupació	
7.3.1 La terminació o el canvi de les responsabilitats d'ocupació	Aplica
8. Gestió d'actius	
8.1 La responsabilitat dels actius	
8.1.1 Inventari d'actius	Aplica
8.1.2 Propietat dels actius	Aplica

8.1.3 Ús acceptable dels actius	Aplica
8.1.4 Categories dels actius	Aplica
8.2 Classificació de la Informació	
8.2.1 Classificació de la informació	Aplica
8.2.2 Etiquetatge de la informació	Aplica
8.2.3 Manipulació dels procediments de control d'actius	Aplica
8.3 Mitjans de manipulació	
8.3.1 Gestió de suports extraïbles	Aplica
8.3.2 Eliminació dels mitjans	Aplica
8.3.3 Transferència de mitjans físics	Aplica
9. Control d'accés	
9.1 Els requisits de negoci de control d'accés	
9.1.1 Política de control d'accés	Aplica
9.1.2 L'accés a les xarxes i serveis de xarxa	Aplica
9.2 Gestió d'accés dels usuaris	
9.2.1 Registre d'usuaris i baixes	Aplica
9.2.2 Accés aprovisionament d'usuaris	Aplica
9.2.3 Gestió de drets d'accés privilegiats	Aplica
9.2.4 Gestió de la informació de connexió de secret dels usuaris	Aplica
9.2.5 Revisió dels drets d'accés dels usuaris	Aplica
9.2.6 L'eliminació o ajust dels drets d'accés	Aplica
9.3 Responsabilitat dels usuaris	
9.3.1 Ús del control de la informació de connexió secreta	Aplica
9.4 Sistema de control i d'accés a les aplicacions	
9.4.1 Restricció d'accés a la informació	Aplica
9.4.2 Procediments de registre en-Secure	Aplica
9.4.3 Sistema de gestió de contrasenyes	Aplica
9.4.4 Ús dels programes de serveis públics privilegiats	Aplica
9.4.5 Control d'accés al codi font del programa	Aplica
10 Criptografia	
10.1 controls criptogràfics	
10.1.1 Política sobre l'ús de controls criptogràfics	Aplica
10.1.2 Gestió de claus	Aplica
11 La seguretat física i ambiental	
11.1 Les àrees segures	
1.1.1 perímetre de seguretat física	Aplica
11.1.2 controls d'entrada físiques	Aplica
11.1.3 Protecció d'oficines, sales i instal·lacions	Aplica
11.1.4 Protecció contra amenaces externes i ambientals	Aplica
11.1.5 El treball en àrees segures	Aplica
11.1.6 Lliurament i càrrega de les zones	Aplica
11.2 Equip	
11.2.1 Emplaçament i la protecció de l'equip	Aplica
11.2.2 Suport als serveis públics	Aplica
11.2.3 La seguretat de cablejat	Aplica

11.2.4 El manteniment de l'equip	Aplica
11.2.5 Eliminació dels actius	Aplica
11.2.6 Seguretat dels equips i actius fora de l'establiment	Aplica
11.2.7 L'eliminació segura o la reutilització dels equips	Aplica
11.2.8 Equip d'usuari desatesa	Aplica
11.2.9 Esborrar escriptori i la política de pantalla transparent	Aplica
12 Operacions de Seguretat	
12.1 Procediments i responsabilitats operacionals	
12.1.1 procediments operacionals, adequadament documentats	Aplica
12.1.2 Gestió de canvis	Aplica
12.1.3 Capacitat de gestió	Aplica
12.1.4 Separació de desenvolupament, prova i entorns operatius	Aplica
12.2 Protecció contra el malware	
12.2.1 Controls contra el malware	Aplica
12.3 Còpia de seguretat	
12.3.1 Informació de còpia de seguretat	Aplica
12.4 Registre i supervisió	
12.4.1 registre d'esdeveniments	Aplica
12.4.2 Protecció de la informació de registre	Aplica
12.4.3 Administrador i operador registres	Aplica
12.4.4 Sincronització del rellotge	Aplica
12.5 de control de programari operacional	
12.5.1 Instal·lació de programari en sistemes operatius	Aplica
12.6 La gestió tècnica de la vulnerabilitat	
12.6.1 Gestió de vulnerabilitats tècniques	Aplica
12.6.2 Restriccions en la instal·lació del programari	Aplica
12.7 Sistemes d'informació consideracions d'auditoria	
12.7.1 Sistemes d'informació controls d'auditoria	Aplica
13 Seguretat de les comunicacions	
13.1 de gestió de seguretat de xarxa	
13.1.1 controls de xarxa	Aplica
13.1.2 Seguretat dels serveis de xarxa	Aplica
13.1.3 La segregació a les xarxes	Aplica
13.2 La transferència d'informació	
13.2.1 polítiques i procediments de transferència d'informació	Aplica
13.2.2 Els acords sobre la transferència d'informació	Aplica
13.2.3 La missatgeria electrònica	Aplica
13.2.4 Confidencialitat o de no divulgació acords	Aplica
14 Sistema d'adquisició, desenvolupament i manteniment	
14.1 Els requisits de seguretat dels sistemes d'informació	
14.1.1 Informació d'anàlisi de requisits de seguretat i les especificacions	Aplica
14.1.2 serveis d'aplicacions de fixació de les xarxes públiques	Aplica
14.1.3 Protecció de les transaccions de serveis d'aplicacions	Aplica
14.2 Seguretat en els processos de desenvolupament i suport	

14.2.1 política de desenvolupament segur	Aplica
14.2.2 els procediments de control de canvis del Sistema	Aplica
14.2.3 Revisió tècnica d'aplicacions després de canvis en la plataforma d'operació	Aplica
14.2.4 Les restriccions als canvis en els paquets de programari	Aplica
14.2.5 principis d'enginyeria de sistemes segurs	Aplica
14.2.6 entorn de desenvolupament segur	Aplica
14.2.7 Desenvolupament externalitzat	Aplica
14.2.8 Les proves de seguretat del sistema	Aplica
14.2.9 Sistema de proves d'acceptació	Aplica
14.3 Les dades de prova	
14.3.1 Protecció de dades de prova	Aplica
15 Les relacions amb proveïdors	
15.1 Seguretat de la informació en relació amb els proveïdors	
15.1.1 La política de seguretat de la informació de relacions amb els proveïdors	Aplica
15.1.2 Abordar la seguretat dins dels acords amb proveïdors	Aplica
15.1.3 Cadena de la tecnologia d'informació i comunicació de subministrament	Aplica
15.2 La gestió de la prestació de serveis de proveïdors	
15.2.1 Seguiment i revisió dels serveis de proveïdors	Aplica
15.2.2 Gestió de canvis en els serveis de proveïdors	Aplica
16 Gestió d'incidents de seguretat d'informació	
16.1 Gestió dels incidents de seguretat de la informació i millores	
16.1.1 Responsabilitats i procediments	Aplica
16.1.2 Informes esdeveniments de seguretat de la informació	Aplica
16.1.3 Informes debilitats de seguretat d'informació	Aplica
16.1.4 L'avaluació i la decisió sobre els esdeveniments de seguretat d'informació	Aplica
16.1.5 Resposta a incidents de seguretat d'informació de control	Aplica
16.1.6 Aprenent dels incidents de seguretat de la informació	Aplica
16.1.7 Reunió de proves	Aplica
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	
17.1 La continuïtat seguretat de la informació	
17.1.1 Planificació de la continuïtat seguretat de la informació	Aplica
17.1.2 Implementació de la informació de seguretat de continuïtat	Aplica
17.1.3 Verificar, revisar i avaluar la informació de seguretat de continuïtat	Aplica
17.2 Les redundàncies	
17.2.1 Disponibilitat d'instal·lacions de processament d'informació	Aplica
18 Compliment	
18.1 El compliment dels requisits legals i contractuals	
18.1.1 Identificació de la legislació aplicable i els requisits contractuals	Aplica
18.1.2 Drets de propietat intel·lectual	Aplica
18.1.3 Registres de control de registres	Aplica
18.1.4 Privacitat i protecció de dades personals	Aplica
18.1.5 Regulació de controls criptogràfics	Aplica
18.2 opinions seguretat de la informació	
18.2.1 Revisió independent de la seguretat de la informació	Aplica

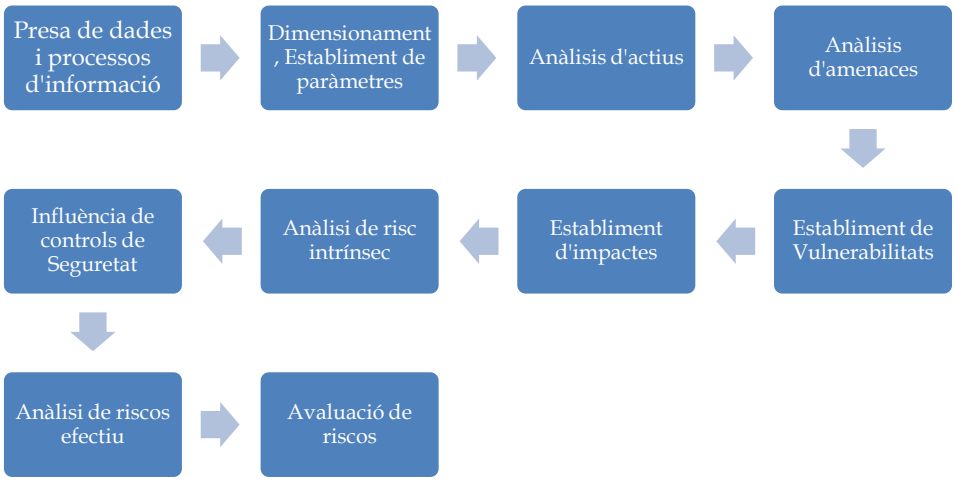
18.2.2 El compliment de les polítiques i normes de seguretat	Aplica
18.2.3 Revisió de compliment tècnic	Aplica

7. Anàlisis de Riscos

7.1. Introducció

La metodologia utilitzada per a execució de l'anàlisi de riscos es basa en la metodologia d'anàlisi de riscos de sistemes d'informació de MAGERIT v.3

Magerit segueix un procés fins a arribar a elaborar i identificar tots els riscos d'una organització. Les fases són les següents:



Imatge 3. Procés per elaborar tots els riscos

Els elements que es tenen en consideració en el procés d'anàlisi de riscos són els següents:

- **Actius**: són tots els elements que té l'organització i que s'analitzen durant el procés. Cal destacar que per a actiu s'entén tot element que requereix l'organització per a fer les activitats de negoci que li són pròpies.
- **Amenaces**: són totes les situacions que poden arribar a passar en una organització i que poden danyar els actius, i provocar, doncs, que aquests actius no funcionin correctament o que no es puguin utilitzar de la manera correcta per a dur a terme l'activitat de negoci de l'organització.
- **Vulnerabilitats**: són les diferents debilitats que presenten els actius identificats anteriorment i que són aprofitats per les amenaces per a provocar un dany.
- **Impactes**: són les conseqüències que es produeixen en l'organització quan una amenaça aprofita una vulnerabilitat per a danyar un actiu.

7.2. Inventari d'actius

Els actius considerats en aquest anàlisi, són aquells elements del Sistema de la Informació necessaris per a l'activitat del negoci.

Els actius s'han classificat segons les seves característiques, per les diferents topologies:

- **Instal·lacions:** Són tots els elements que té l'organització i que necessita perquè la resta funcioni correctament. Són, per exemple, els sistemes d'aire condicionat o el cablejat de dades i de corrent elèctric.
- **Hardware:** Són tots els elements de tipus *maquinari* que s'utilitzen en l'organització: ordinadors, servidors, portàtils, PDA, telèfons mòbils, impressores, etc.
- **Aplicació i software:** Són tots els elements de *programari* que s'utilitzen: sistemes operatius, aplicacions pròpies, etc.
- **Dades:** Són els elements que contenen la informació que permet a una organització prestar els seus serveis: fitxers, BBDD, copies de seguretat, etc.
- **Xarxa:** Són tots els elements que transporten dades d'un lloc a un altre: Internet, routers, xarxes sense fil WiFi, telefonia mòbil, etc.
- **Serveis:** Són els elements que satisfà una necessitat als usuaris.
- **Equipament auxiliar:** Són els elements que estan relacionats directament amb el tractament de dades. Per exemple: sistemes de refrigeració, sistemes d'alimentació ininterrompuda, cablejat, robots de cinta, caixes fortes, equips de destrucció, etc.
- **Personal:** Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització: responsable de seguretat, administrador de la xarxa, personal d'administració, secretaris, usuaris, etc.

A continuació detallem una taula a mode resum, per veure l'inventari amb detall aneu a l'ANNEX VII:

Àmbit	Codi	Actiu
Instal·lacions	I.1	CPD
	I.2	Llocs de treball corporatius
	I.3	Llocs de direcció
	I.4	Llocs de treball divisió d'operació
	I.5	Llocs de treball divisió industrial
	I.6	Llocs de treball comercial
	I.7	Sales d'impressió
Hardware	HW.1	Firewalls
	HW.2	Proxys
	HW.3	Siem
	HW.4	IPS
	HW.5	Qualys
	HW.6	Load Balancer
	HW.7	Routers
	HW.8	Impresores
	HW.9	Workstations
	HW.10	Laptops
	HW.11	Mòbils

	HW.12	AIX 6
	HW.13	Cabina de discos SATA – Dades
	HW.14	VMWARE ESXi
	HW.15	Backups
	HW.16	Commutadors xarxa
Aplicació i software	SW.1	SCADA
	SW.2	Windows 7
	SW.3	Windows Server 2003
	SW.4	Windows server 2008 R2
	SW.5	Windows server 2012 R2
	SW.6	Red Hat Enterprise Linux 5.9
	SW.7	Red Hat Enterprise Linux 6.5
	SW.8	Red Hat Enterprise Linux 6.7
	SW.9	Apache Tomcat
	SW.10	IIS
	SW.11	SQL
	SW.12	Oracle 10g
	SW.13	Oracle 11g
	SW.14	Oracle 12c
	SW.15	Solaris 11
	SW.16	AD RHH
	SW.17	SAP
	SW.18	Antivirus
	SW.19	HP Data Protector
Dades	D.1	Backups
	D.2	Documentum
	D.3	DMS
	D.4	GDS
Xarxa	X.1	ADSL
	X.2	Routers Wifi
Serveis	S.1	GDS
	S.2	AD RRHH
	S.3	Impresores
	S.4	Exchange
	S.5	Webs
	S.6	Viatjes
	S.7	Formació
Equipament auxiliar	EA.1	Armaris rack CPD
	EA.2	Refrigeració CPD
	EA.3	Side
Personal	P.1	Director TI
	P.2	Responsable de Riscos

	P.3	Tècnics INTEL
	P.4	Tècnics UNIX
	P.5	Tècnics web
	P.6	Tècnics BBDD
	P.7	Tècnics SAP
	P.8	Tècnics de Xarxes
	P.9	Tècnics d'operacions
	P.10	Tècnics de monitoring
	P.11	Tècnics de backup
	P.12	Tècnics Seguretat i antivirus
	P.13	Tècnics de desenvolupament
	P.14	Tècnics Acive Directory
	P.15	Tècnics SCCM

7.3. Valoració dels actius

En aquesta fase de Magerit assignarem una valoració econòmica a tots els actius d'una organització que es pretenen analitzar. Els actius que analitzarem són els que requereix l'organització per a dur a terme els processos que són propis d'aquesta organització.

Primer de tot definim els rangs econòmics segons la valoració dels actius, a continuació detallem el valor econòmic segons la valoració de l'actiu:

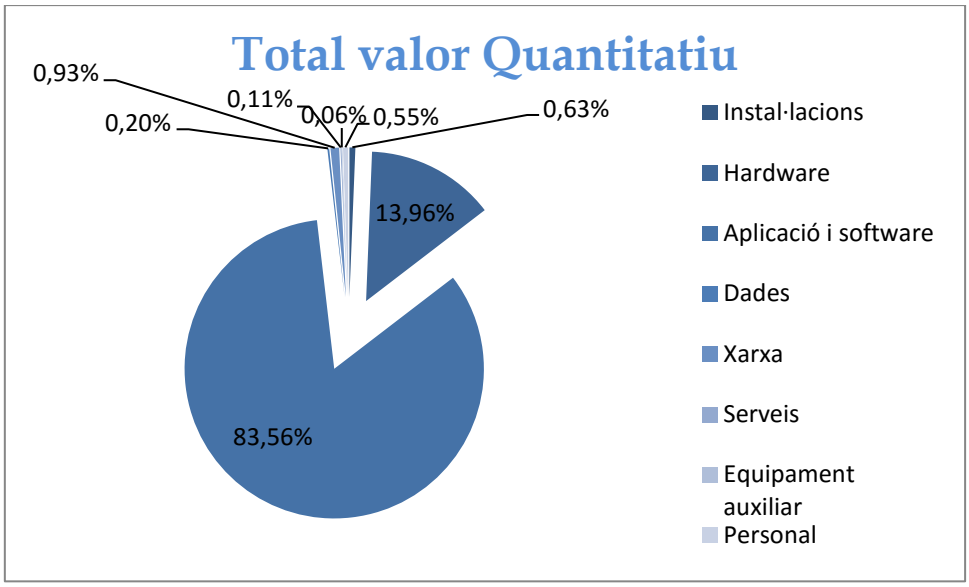
Valoració d'actius		
Descripció	**Abreviatura**	**Valor**
Molt alt	MA	300.000
Alt	A	150.000
Mitjà	M	75.000
Baix	B	30.000
Molt baix	MB	10.000
Menyspreable	D	5.000

A l'hora d'assignar una valoració a cada actiu tindrem en consideració el següent:

- El **valor de reposició**: és el valor que té per a l'organització reposar aquest actiu en cas que es perdi o que no es pugui utilitzar.
- El **valor de configuració**: és el temps que es necessita des que s'adquireix el nou actiu fins que es configura o es posa a punt perquè es pugui utilitzar per a la funció que desenvolupava l'anterior actiu.
- El **valor d'ús de l'actiu**: és el valor que perd l'organització durant el temps que no pot utilitzar aquest actiu per a la funció que desenvolupa.
- El **valor de pèrdua d'oportunitat**: és el valor que perd potencialment l'organització pel fet de no poder disposar d'aquest actiu durant un temps.

A continuació detallem els resultats de la valoració d'actius a mode resum, per veure la taula completa de la valoració d'actius aneu a l'ANNEX VII:

Àmbit	Total valor Quantitatiu
Instal·lacions	14.030.000
Hardware	308.375.000
Aplicació i software	1.846.285.000
Dades	4.350.000
Xarxa	2.047.5000
Serveis	2.450.000
Equipament auxiliar	1.380.000
Personal	12.180.000
Total	**2.209.525.000**



Gràfica 4. Valor Quantitatiu dels actius de Traun

7.4. Dimensions de seguretat

Des de el punt de vista de la seguretat, s'ha d'indicar quin es l'aspecte de la seguretat més crític. Aquesta valoració mesura la cripticitat a les cinc dimensions de la seguretat de la informació manegada pel procés de negoci. A continuació detallem les cinc dimensions:

- **Disponibilitat**: Propietat o característica dels actius consistent en que les entitats o processos autoritzats tenen accés als actius quan ho requereixen. Un

actiu no té valor apreciable si pot romandre no disponible freqüentment o durant llargs períodes. Afecta a tot tipus d'actius.

- **Integritat**: característica que indicaria que l'actiu d'informació no ha estat alterat de manera no autoritzada. Si la seva alteració no suposa cap preocupació, el seu valor serà menyspreable.
- **Confidencialitat**: propietat consistent en que la informació ni es posa a disposició ni es revela a individus, entitats o processos no autoritzats. Si es valora que la revelació provocaria un greu perjudici a l'entitat o organització, obtindrà un valor alt.
- **Autenticitat**: propietat consistent en que una entitat, individu o procés és qui diu ser, o bé garanteix la font origen de les dades. Si un servei prestat a usuaris no autenticats pot provocar un greu perjudici, la dimensió d'autenticitat obtindrà un valor alt. També pot ser-ho si el fet que la font origen de les dades és el que hauria pot provocar un perjudici greu.
- **Traçabilitat**: característica consistent en que les actuacions d'una entitat poden ser imputades a aquesta entitat o subjecte.

Un cop explicades les cinc dimensions, s'ha de tenir present l'escala a la que es realitzaran les valoracions. En aquest cas utilitzarem una escala de valoració de deu valors, seguint els següents criteris:

CRITERI	CRITERI
10	Dany molt greu a la organització
7-9	Dany greu a la organització
4-6	Dany important a la organització
1-3	Dany menor a la organització
0	Dany irrellevant a la organització

Per veure la valoració realitzada, veieu l'ANNEX VII.

7.5. Anàlisi d'amenaces

Realitzarem una estimació de l'impacte de les possibles amenaces sobre els actius, aproximant el seu valor de probabilitat de materialització. Cada amenaça pot provocar un possible impacte en una o més de les diferents dimensions de seguretat de l'actiu.

La metodologia utilitzada agrupa les amenaces a les següents categories:

- **Amenaces d'origen natural:** accidents naturals com terratrèmols, inundacions, etc.
- **Amenaces d'entorn o d'origen industrial:** Incidents que solen produir-se de manera accidental, que tenen el seu origen en elements de tipus industrial, com la contaminació o les fallades elèctriques.

- **Errors i errors no intencionats**: Errors no intencionals causats per les persones, típicament per error o per omissió.
- **Atacs intencionats:** Fallades deliberats causats per les persones, bé amb ànim de beneficiar indegudament, bé amb ànim de causar danys i perjudicis.

Per veure amb detall la identificació d'amenaces aneu a l'ANNEX VIII.

Un cop s'han establert i identificar les amenaces, s'ha de realitzar una valoració de la seva influència en el valor dels actius. En aquesta anàlisi s'ha avaluat la freqüència:

- **La vulnerabilitat**: Determinada segons la freqüència (quan probable o improbable) que es materialitza una amenaça.

Freqüència			
Descripció	**Rang**	**Abreviatura**	**Valor**
Extremadament freqüent	1 vegada al dia	EF	1
Molt freqüent	1 vegada cada dos setmanes	MF	0,071232877
Freqüent	1 vegada cada dos mesos	F	0,016438356
Poc Freqüent	1 vegada cada quatre mesos	PF	0,010958904
Molt poc freqüent	1 vegada cada 6 mesos	MPF	0,005479452
Menyspreable	1 vegada a l'any	D	0,002739726

Per veure amb detall la freqüència d'actius vs amenaces aneu a l'ANNEX IX.

7.6. Impacte potencial

El primer element a calcular és **l'Impacte Potencial**, que identificarà la magnitud del dany que podria causar en l'organització el fet que arribes a ocórrer alguna de les amenaces.

Impacte Potencial = Valor de l'actiu x Impacte

Per poder realitzar aquest càlcul s'ha utilitzat:

- El valor de cada un dels actius i per a totes les seves dimensions, calculat en apartats anteriors, per veure la valoració realitzada, veieu l'ANNEX VII.

- **L'impacte**: Per a Magerit, s'entén per impacte el tant per cent del valor de l'actiu que es perd en cas que hi hagi una incidència sobre aquest actiu. Per veure l'impacte vs actius consultar l'ANNEX X.

Impacte		
Descripció	Abreviatura	Valor
Crític	C	90%
Alt	A	75%

Mitjà	M	50%
Baix	B	20%

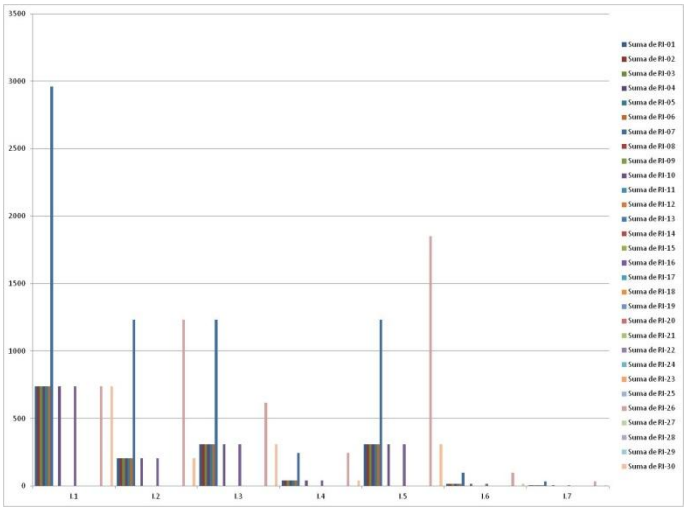
El segon element a calcular és el Risc Intrínsec, risc al qual l'actiu està exposat sense tenir en consideració les mesures de seguretat implantades.
Per analitzar del **risc intrínsec**, s'ha utilitzat:

- El valor de l'Impacte Potencial, calculat anteriorment, per veure la valoració realitzada veieu l'ANNEX X.
- La Freqüència que pot ocórrer una amenaça calculat en apartats anteriors, per veure la valoració realitzada veieu l'ANNEX IX.

Risc Intrínsec = Impacte Potencial x Freqüència

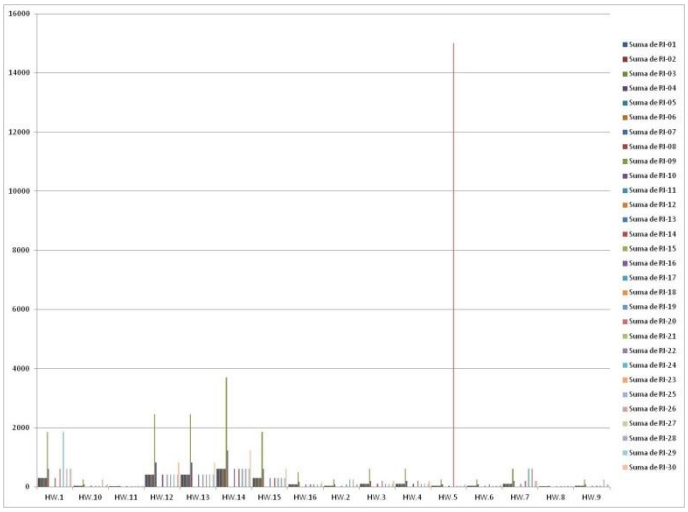
A l'ANNEX VII trobarem el risc intrínsec de tots els actius segons la freqüència de les amenaces. A continuació mostrem unes taules resum segons cada categorització dels actius:

Risc Intrínsec dels actius categoritzats com Instal·lacions:



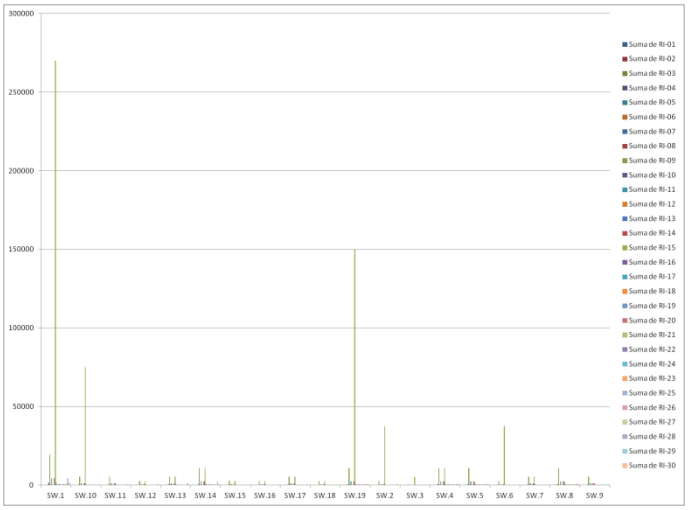
Gràfica 5. Risc Intrínsec dels actius categoritzats com Instal·lacions

Risc Intrínsec dels actius categoritzats com **Hardware:**



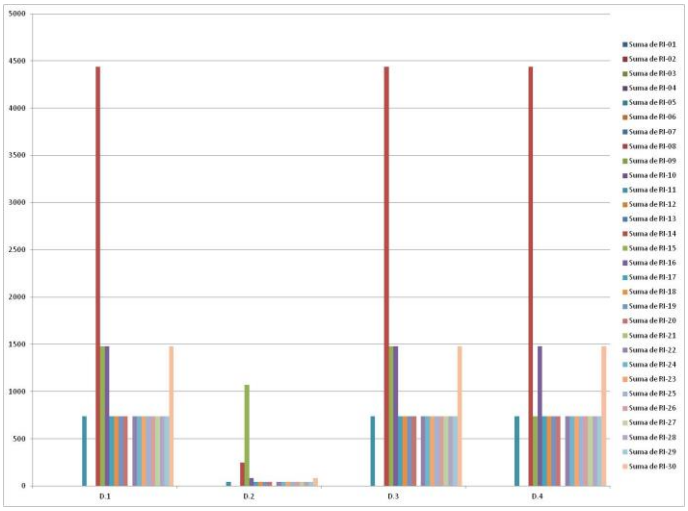
Gràfica 6. Risc Intrínsec dels actius categoritzats com Hardware

Risc Intrínsec dels actius categoritzats com Aplicació i software



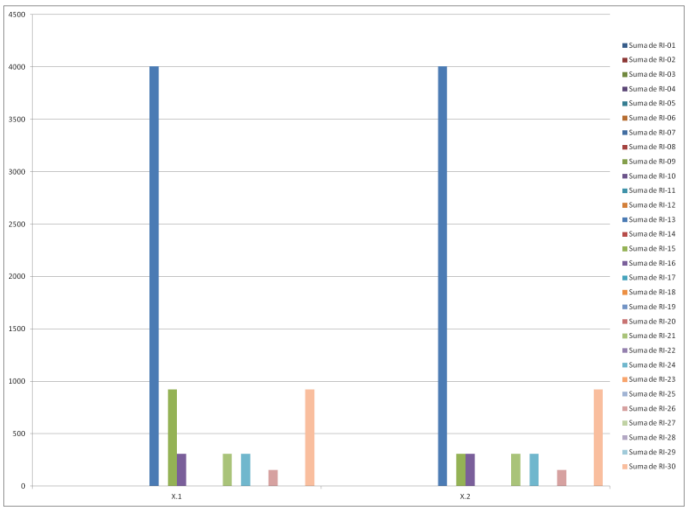
Gràfica 7. Risc Intrínsec dels actius categoritzats com Software

Risc Intrínsec dels actius categoritzats com **Dades:**



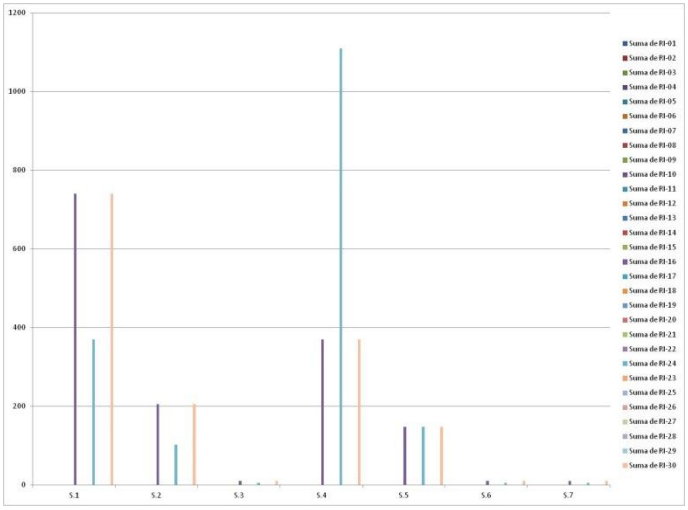
Gràfica 8. Risc Intrínsec dels actius categoritzats com Dades

Risc Intrínsec dels actius categoritzats com **Xarxa:**



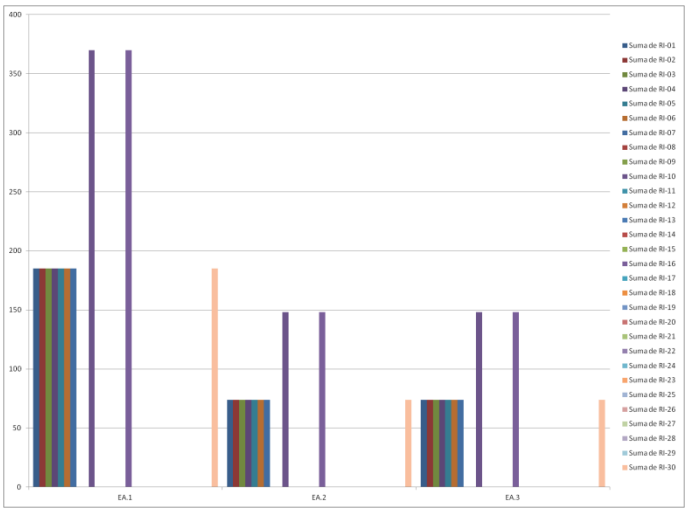
Gràfica 9. Risc Intrínsec dels actius categoritzats com Xarxes

Risc Intrínsec dels actius categoritzats com **Serveis:**



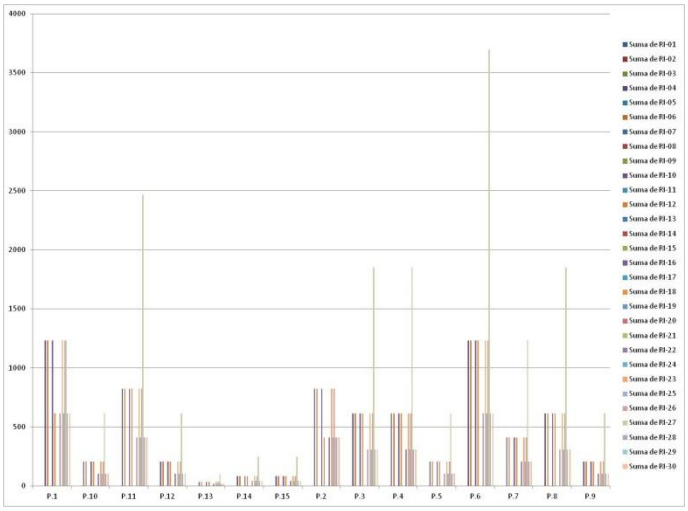
Gràfica 10. Risc Intrínsec dels actius categoritzats com Serveis

Risc Intrínsec dels actius categoritzats com Equipament auxiliar:



Gràfica 11. Risc Intrínsec dels actius categoritzats com Equipament auxiliar

Risc Intrínsec dels actius categoritzats com **Personal:**



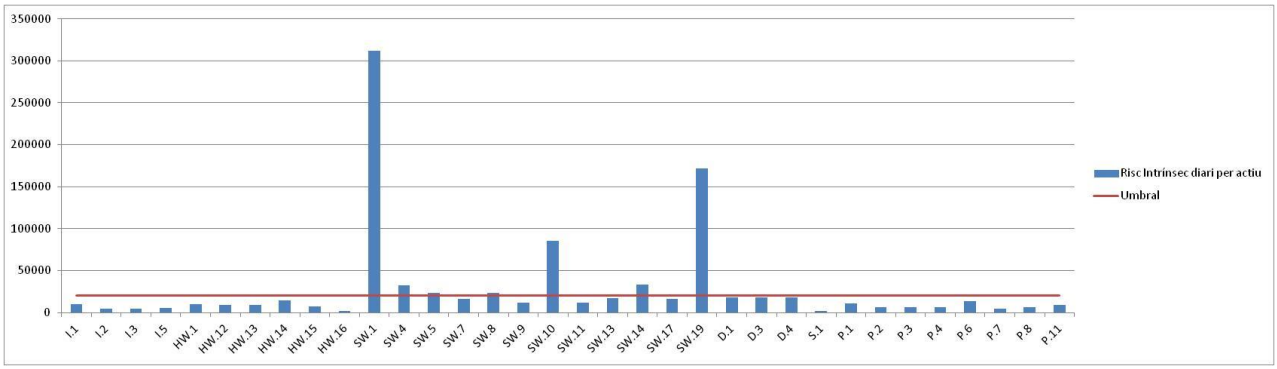
Gràfica 12. Risc Intrínsec dels actius categoritzats com Personal

7.7. Nivell de Risc Acceptable i Risc Residual

Un cop realitzat tots els càlculs, l'organització ha de determinar quin nivell de risc està disposada a assumir i qual decideix mitigar mitjançant l'aplicació de controls de seguretat.

- El Risc Acceptable: és el risc que ha quedat per sota del llindar marcat per l'Organització.
- El Risc Residual: és el risc romanent després d'haver desplegat el conjunt de mesures de seguretat.

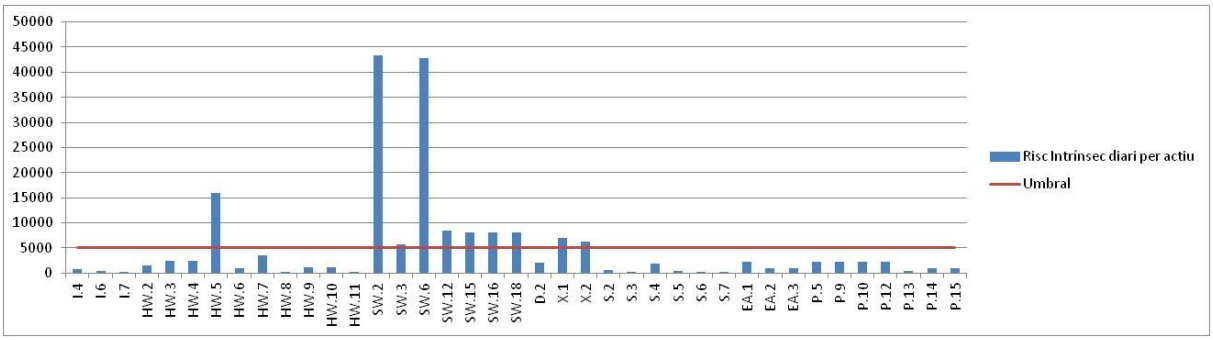
Traun ha de definir un llindar, el qual és el límit dels riscos que estan disposats assumir. S'ha prioritzat els actius valorats com "Molt Alt"(MA) i "Alt"(A), el umbral econòmic definit per aquest actius es de **20.000 euros**.



Gràfica 13. Risc intrínsec amb els actius amb valor alt i molt alt

A continuació en els resultats veurem els actius (MA,A) per sobre de l'umbral amb més detall.

Per als actius amb valor "Mitjà" (M), "Baix" (B), "Molt baix" (MB) i "Menyspreable" (D), el umbral econòmic es de **5.000 euros**, aquest valor es el que esta disposat assumir Traun.



Gràfica 14. Risc intrínsec amb els actius amb valor mig, baix i molt baix.

A continuació en els resultats veurem els actius (M,B,MB,D) per sobre de l'umbral amb més detall.

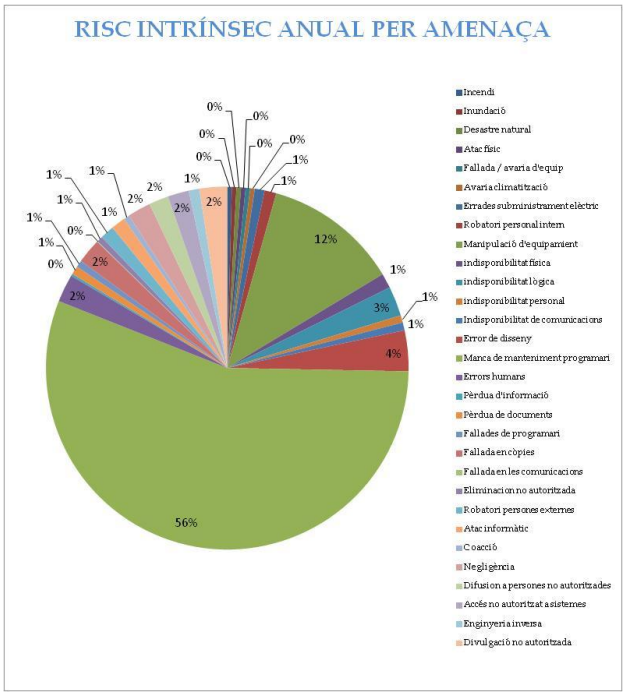
7.8. Resultats

En l'Anàlisi de Riscos hem pogut determinar els actius que són més crítics per a Traun, les amenaces que poden afectar-los i finalment el Risc Intrínsec al qual estan exposats, i sobretot el risc acceptable que esta disposat assumir l'organització.

A continuació mostrem una gràfica del risc intrínsec per amenaça, on observem que les principal amenaces a les quals ens afrontem són:

- Manca de manteniment programari→56%
- Manipulació d'equipament→ 12%
- Error de disseny→4%

El principal risc es la manca de manteniment de programari, ens troben en una organització on el seu producte es realitza a les fàbriques, on encara no s'ha actualitzar ni realitzat millores del programari, fins a dia d'avui, encara no era gestionat per l'àrea IT, són els treballadors de la fàbrica qui "manté" els actius, software, hardware més importants per a l'organització.

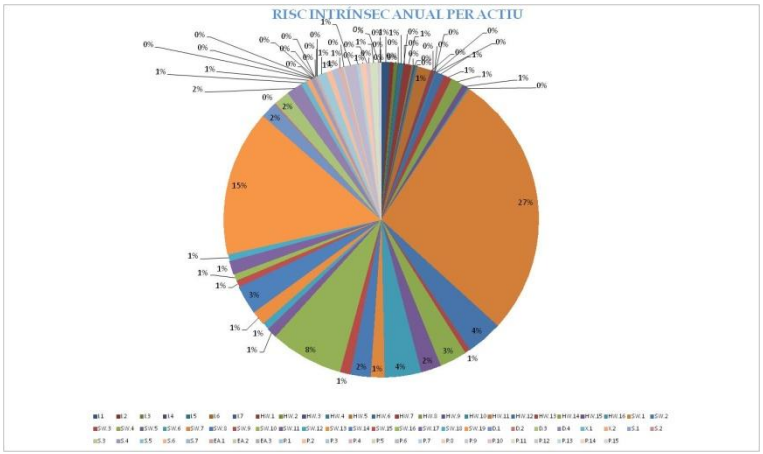


Gràfica 15. Risc Intrínsec anual per amenaça

A continuació mostrem una gràfica del risc intrínsec per actiu, on observem que els principals actius amb més amenaces són:

- SW.1 SCADA→27%
- SW.19 HP Data Protector → 15%
- SW.10 IIS →8%

Els actius amb més prioritat a l'empresa són els que a dia d'avui tenen més amenaces, en el cas de SCADA, tal i com la gràfica anterior s'indicava, aquest es gestionat i administrat per la part de fàbrica.
El HP Data Protector, ens trobem amb el mateix cas, la pròpia eina de IT per realitzar backups, ens trobem amb la manca de manteniment del programari, i estem en procés de migració.



Gràfica 16. Risc Intrínsec anual per actiu

Veurem els resultats dels actius els quals no es troben dins del risc acceptable i els quals l'organització haurà de prendre mesures:

A continuació els actius amb valor M,B,MB i D:

Codi	Actiu	Valor Qualitatiu	Risc Intrínsec diari per actiu
HW.5	Qualys	M	15904,10959
SW.2	Windows 7	M	43253,42466
SW.3	Windows Server 2003	MB	5712,328767
SW.6	Red Hat Enterprise Linux 5.9	M	42842,46575
SW.12	Oracle 10g	M	8424,657534
SW.15	Solaris 11	M	8013,69863
SW.16	AD RHH	M	8013,69863
SW.18	Antivirus	M	8013,69863
X.1	ADSL	M	6934,931507
X.2	Routers Wifi	M	6318,493151

Els riscos principals que afecten aquests actius i que hauran de ser mitigats sobre els actius mitjans són:

- Manipulació d'equipament
- Manca de manteniment programari
- Error de disseny

A continuació els actius amb valor MA i A:

Codi	Actiu	Valor Qualitatiu	Risc Intrínsec diari per actiu
SW.1	SCADA	MA	312164,3836
SW.4	Windows server 2008 R2	MA	32054,79452
SW.5	Windows server 2012 R2	MA	23835,61644
SW.8	Red Hat Enterprise Linux 6.7	MA	23835,61644
SW.10	IIS	A	85890,41096
SW.14	Oracle 12c	MA	33698,63014
SW.19	HP Data Protector	MA	171369,863

Els riscos principals que afecten aquests actius i que hauran de ser mitigats sobre els actius crítics són:

- Manca de manteniment programari
- Manipulació d'equipament
- Error de disseny

En tots els anàlisi podem observar que els principals problemes de l'organització són:

- La manca de manteniment de programari, hi ha un gran treball a fer i el principal es realitzar una CMDB amb tots els actius de l'Organització.
- Centralitzar tot els software, hardware, etc en IT. Reorganització i segregació de funcions, inclòs SCADA.
- Millorar l'antivirus, degut a que les petites seus distribuïdes mundialment son un gran focus d'infecció diària per diferents tipus de malware.
- Actualització de sofware (Windows, Oracle, etc).
- Falta d'implementació d'un procediment de backups amb un software actual.
- Millorar les instal·lacions del principal CPD d'Espanya.
- Millora del procés de pegats i auditories de compliment normatiu, Qualys.

8. Propostes de Projectes

8.1. Introducció

El Sistema de Gestió de la Seguretat de la Informació, en endavant SGSI, es el procés de millora continua de les amenaces a les que estan exposades Traun. En la fase anterior s'han determinat els riscos els quals està exposada l'Organització i en conseqüència, les necessitats en matèria de seguretat.
En aquest apartat seleccionarem i prioritzarem una sèrie de mesures en forma de projectes que permetin millorar la seguretat de Traun.
És important realitzar una renovació i actualització de les mesures de seguretat, seguint el cicle Deming (PDCA), incrementant el nivell de maduresa de l'anàlisi de riscos, per prendre-ho com a punt de partida en la selecció dels projectes de seguretat, alineant amb els objectius de l'Organització.

Mitjançant aquesta progressió sobre el SGSI i el control del risc s'aconseguirà un compliment adequat de la norma ISO/IEC 27001: 20013

El pla d'execució i implantació dels diferents projectes es contempla dins d'un període de tres anys, corresponent amb el cicle de la ISO 27001. S'han definit tres fases d'execució o implantació durant els quals es duran a terme les diferents implementacions dels projectes:

- Projectes a **curt** termini: realització e implantació durant el primer any.
- Projectes a **mig** termini: realització e implantació durant el segon any.
- Projectes a **llarg** termini: realització e implantació durant el tercer any.

8.2. Propostes

8.2.1. Projectes a curt termini

A continuació es presenten els projectes a implantar durant el primer any:

- ITINF105:Realització de l'inventari d'actius (CMDB).
- ITINF212: Implementació advanced threat detection (ATD).
- ITINF045: Programa de conscienciació sobre la seguretat.
- ITINF150: Implementació de pegats Red Hat.
- ITINF151: Actualització del sofware de backups.
- ITINF065: Millora dels Centre de Processament de Dades (Migració).

Per entrar en més detall sobre els projectes a curt termini, veure l'ANNEX XI.

8.2.2. Projectes a mig termini

A continuació es presenten els projectes a implantar durant el segon any:

- ITINF068: Implementació Policy Compliance, auditories de compliment normatiu.
- ITINF090: Procés de gestió de backups
- ITINF220: Migració Windows 2003 a Windows server 2012
- ITINF221: Migració Oracle 10g a Oracle 12c

Per entrar en més detall sobre els projectes a mig termini, veure l'ANNEX XII.

8.2.3. Projectes a llarg termini

A continuació es presenten els projectes a implantar durant el tercer any:

- ITINF025: Procediments i gestió d'auditories internes i externes.
- ITINF085: Reestructuració del departament TIC.

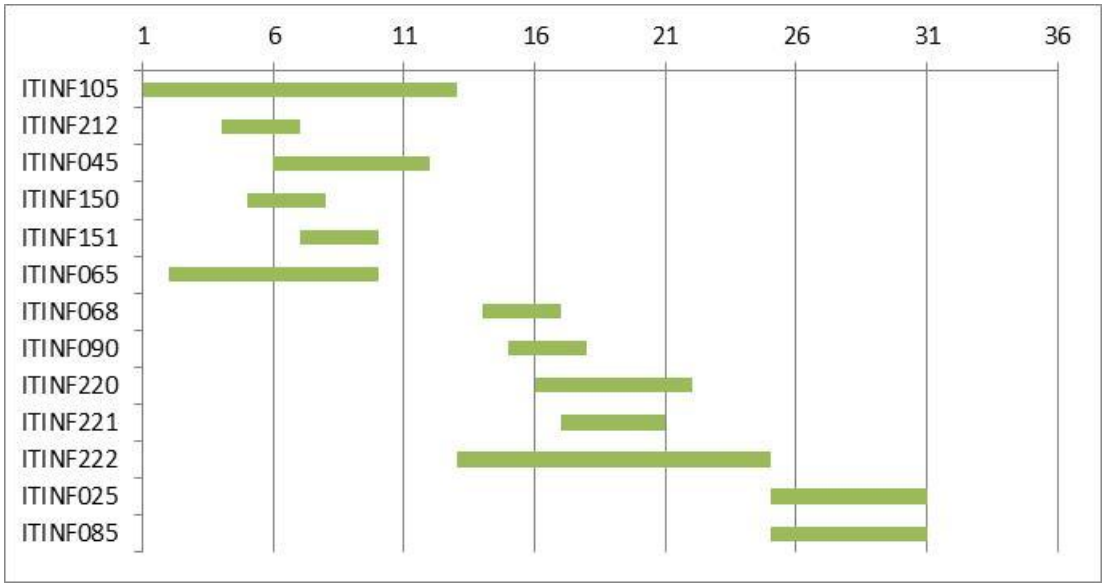
Per entrar en més detall sobre els projectes a llarg termini, veure l'ANNEX XIII.

8.3. Resultats

Un cop definits tots els projectes planificats per cadascun dels períodes, realitzem un resum dels resultats obtinguts :

- Segons l'anàlisi de riscos
- Segons la ISO27001

A continuació la planificació definida per l'execució dels diferents projectes:



Gràfica 17. Planificació amb la gràfica Grant

És resumeix les despeses a realitzar per part de l'organització per cadascun dels projectes:

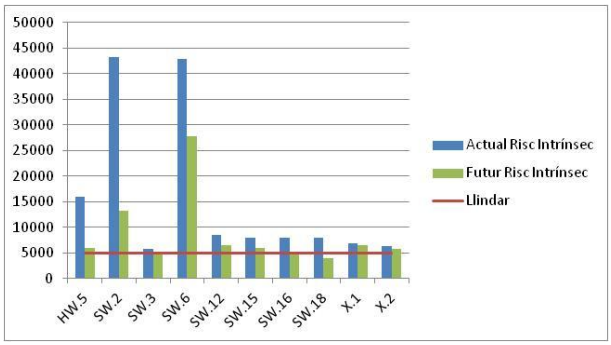
Períodes	Projecte	Duració	Inici	Fi	Cost total
Curt Termini	ITINF105	12 mesos	15/01/2016	31/12/2016	7.460€
	ITINF212	3 mesos	01/04/2016	01/07/2016	1.255€
	ITINF045	6 mesos	01/06/2016	01/12/2016	1.370€
	ITINF150	3 mesos	01/05/2016	01/08/2016	1.760€
	ITINF151	3 mesos	01/07/2016	01/10/2016	1.510€
	ITINF065	8 mesos	01/02/2016	01/10/2016	8.980€
Mig Termini	ITINF068	3 mesos	27/02/2017	27/05/2017	1.530€
	ITINF090	3 mesos	01/03/2017	01/06/2017	1.440€
	ITINF220	6 mesos	01/04/2017	01/10/2017	2.870€
	ITINF221	4 mesos	01/05/2017	01/09/2017	990€
Llarg Termini	ITINF025	6 mesos	01/01/2018	01/06/2018	1.370€
	ITINF085	6 mesos	01/01/2018	01/06/2018	12.050€

8.3.1. Evolució del risc

L'elecció d'aquests projectes s'ha realitzat amb el propòsit de mitigar els riscos en aquells actius que tenen un nivell de risc superior al llindar establert. A la finalització dels tres anys, havent-se executat correctament tots els projectes, haurem mitigat el risc pels deu actius amb risc més elevat de l'organització.

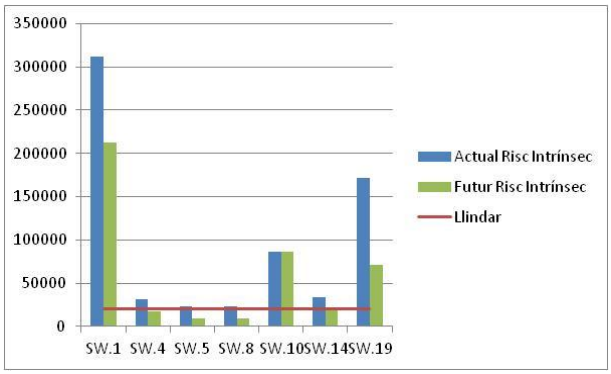
En el pròxim anàlisi de riscos esperem que mostri uns resultats totalment diferents als actuals i d'aquesta manera millorar el risc dels actius en cada cicle PDCA del Sistema de Gestió de Seguretat de la Informació.

A continuació l'evolució que tindrà el risc després de la implementació dels projectes amb els actius amb valor M,B,MB i D:



Gràfica 18.Evaluació Risc intrínsec amb els actius amb valor mis, baix i molt baix

A continuació l'evolució que tindrà el risc després de la implementació dels projectes amb els actius els actius amb valor MA i A:

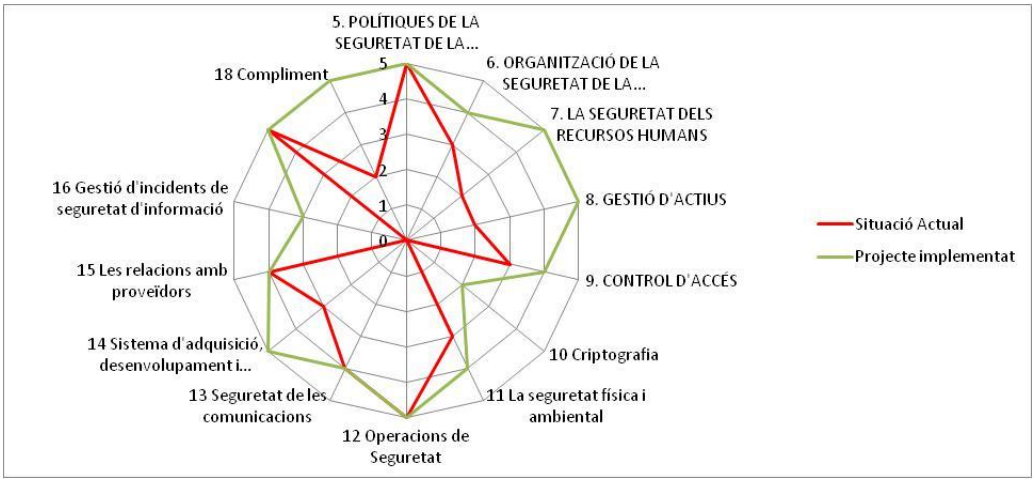


Gràfica 19.Evaluació Risc intrínsec amb els actius amb valor alt i molt alt

8.3.2. Evolució de la norma ISO/IEC 27002:2013

Un cop implantat el SGSI i realitzats els projectes plantejats, l'evolució del compliment es veu millorada àmpliament..

El següent gràfic mostren l'evolució des de l'inici del Pla Director (Gener 2016) fins a la data prevista de finalització dels projectes plantejats (Desembre 2018).



Gràfica 20.Evaluació de la norma ISO/IEC 27002:2013

9. Auditoria de compliment

9.1. Introducció

El cicle de millora contínua (PDCA) en el qual està basat el Sistema de Gestió de la Seguretat de la Informació implantat, s'ha de fer una fase de validació (C) del seu estat i la idoneïtat del seu disseny.

La validació es realitzarà mitjançant una Auditoria de Compliment que proporciona una visió independent del grau de maduresa de la seguretat respecte les ISO. Aquestes auditories s'han de fer amb una periodicitat anual i de planificar dins el Pla d'Auditoria.

Al finalitzar la implementació dels projectes, al desembre del 2018, l'auditoria realitzada té un caràcter inicial i el seu objectiu és revisar el nivell de compliment de les mesures de seguretat implantades respecte els objectius de control que defineix la ISO/IEC 27002: 2013.

Els resultats d'aquesta auditoria proporcionen una sèrie de "No Conformitats" i "Recomanacions" que seran utilitzades per a la fase de millora del SGSI i després d'un termini temporal tornar a revisar aquestes millores.

9.2. Metodologia

Aquesta Auditoria es realitza respecte a als 114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius de control de la i ISO/IEC 27002, i ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

Aquesta valoració la realitzarem segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	**L0**	Inexistent	Carència completa de qualsevol procés que reconeguem.
10%	**L1**	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
50%	**L2**	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
90%	**L3**	Procés definit	La organització sencera participa al procés.
95%	**L4**	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
100%	**L5**	Optimitzat	Els processos estan sota constant millora.

Aquesta auditoria s'ha realitzat seguint les indicacions del Pla d'Auditoria establert, repartint les tasques en tres etapes:

a. Recollida i revisió d'Informació

Durant aquesta etapa es demana tota la documentació i registres rellevants per a l'Auditoria. Un cop recopilada aquesta informació, es revisa la seva idoneïtat i vigència, a més que es trobi alineada amb les bones pràctiques especificades per la ISO.

b. Execució de proves d'Auditoria

Aquesta etapa aglutina el conjunt de tasques que proporcionen la informació necessària per a determinar el grau de compliment.

- Realització d'entrevistes amb responsables i personal.
- Verificació de controls tècnics (implantació i funcionament).
- Realització de Visites per examinar aspectes de seguretat física.

c. Anàlisi de la Informació i Elaboració d'Informes

Durant aquesta etapa, s'analitza la informació recollida en les diferents proves i entrevistes de les anteriors etapes. Aquesta anàlisi ha de determinar el nivell de maduresa i compliment respecte a la ISO, localitzant les fortaleses i les No Conformitats.

Finalment s'elabora un informe per proporcionar la informació rellevant, així com els diferents troballes realitzades.
Per veure amb més detall l'auditoria, en l'ANNEX XIV podeu trobar l'informe d'auditoria pressuposant que hem implementat tots els projectes anteriorment definits.

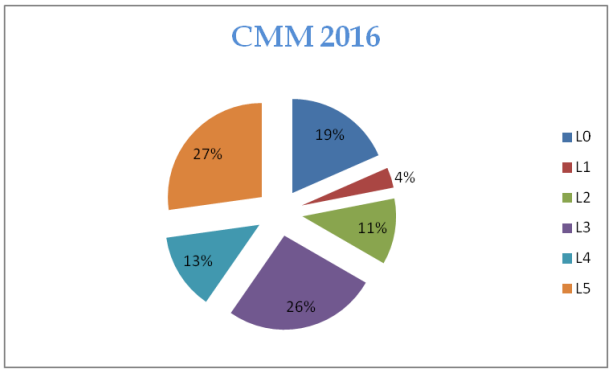
9.3. Avaluació de la maduresa

L'objectiu d'aquesta fase del projecte es avaluar la maduresa de la seguretat, per lo que fa als diferents dominis de control plantejats per la ISO/IEC 27002:2013.

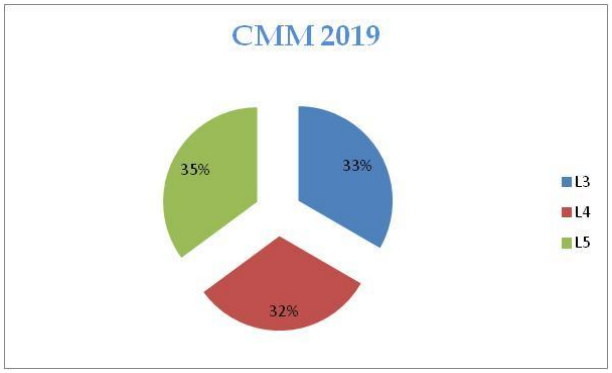
Per realitzar el mesurament del grau de maduresa s'ha utilitzat el model CMM, igual que a la fase d'anàlisis diferencial. On s'estableixen una sèrie de nivells i percentatges que permeten identificar el progrés realitzat en cada un dels controls auditats.

Àrees	CMM 2016	CMM 2019
5. Polítiques de la Seguretat de la Informació	L5	L5
6.Organització de la seguretat de la informació	L3	L4
7. La seguretat dels recursos humans	L2	L5
8. Gestió d'actius	L2	L5
9. Control d'accés	L3	L4
10.Criptografia	L0	L2
11.La seguretat física i ambiental	L3	L4
12.Operacions de Seguretat	L5	L5
13.Seguretat de les comunicacions	L4	L4
14.Sistema d'adquisició, desenvolupament i manteniment	L3	L5

15.Les relacions amb proveïdors	L4	L4
16.Gestió d'incidents de seguretat d'informació	L0	L2
17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	L5	L5
18.Compliment	L2	L4



Gràfica 21. Percentatge de controls segons valor CMM al 2016



Gràfica 22. Percentatge de controls segons valor CMM al 2019

Per veure amb més detall l'auditoria, en l'ANNEX XIV podeu trobar l'informe d'auditoria pressuposant que hem implementat tots els projectes anteriorment definits.

9.4. Resultats

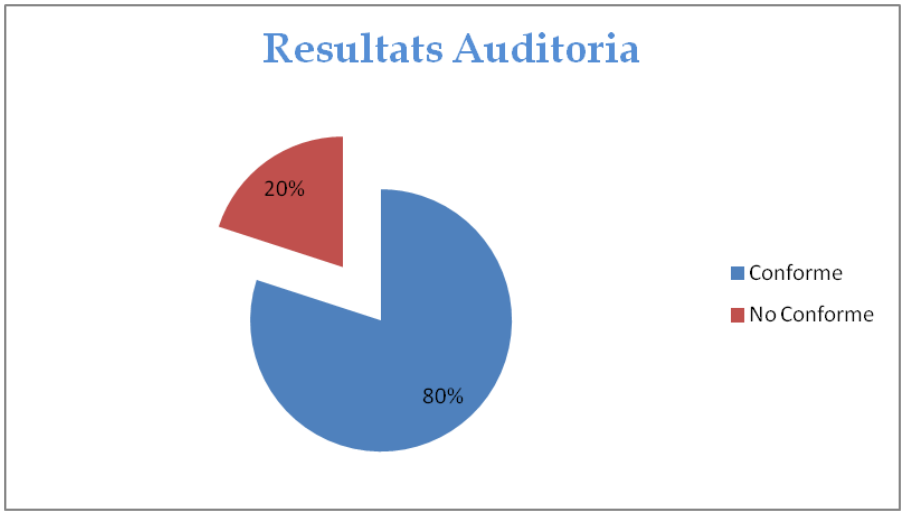
Com a resultat de l'auditoria de cada un dels controls de la ISO27002 de referència s'han trobat un total de 7 "No Conformitats" que hauran de ser corregides.

Aquestes "No Conformitats" es troben en els següents controls de la norma:

- 6.2 Els dispositius mòbils i el teletreball
- 9.1 Els requisits de negoci de control d'accés
- 10.1 Controls criptogràfics
- 11.2 Equip
- 13.2 La transferència d'informació
- 15.1 Seguretat de la informació en relació amb els proveïdors
- 16.1 Gestió dels incidents de seguretat de la informació i millores

Controls	Conformitats
5.1 Direcció de gestió de seguretat de la informació	Conforme
6.1 Organització interna	Conforme
6.2 Els dispositius mòbils i el teletreball	No Conforme
7.1 Amb anterioritat a l'ocupació	Conforme
7.2 Durant l'ocupació	Conforme
7.3 Terminació i canvi d'ocupació	Conforme
8.1 La responsabilitat dels actius	Conforme
8.2 Classificació de la Informació	Conforme
8.3 Mitjans de manipulació	Conforme
9.1 Els requisits de negoci de control d'accés	No Conforme
9.2 Gestió d'accés dels usuaris	Conforme
9.3 Responsabilitat dels usuaris	Conforme
9.4 Sistema de control i d'accés a les aplicacions	Conforme
10.1 Controls criptogràfics	No Conforme
11.1 Les àrees segures	Conforme
11.2 Equip	No Conforme
12.1 Procediments i responsabilitats operacionals	Conforme
12.2 Protecció contra el malware	Conforme
12.3 Còpia de seguretat	Conforme
12.4 Registre i supervisió	Conforme
12.5 de control de programari operacional	Conforme
12.6 La gestió tècnica de la vulnerabilitat	Conforme
12.7 Sistemes d'informació consideracions d'auditoria	Conforme
13.1 De gestió de seguretat de xarxa	Conforme
13.2 La transferència d'informació	No Conforme
14.1 Els requisits de seguretat dels sistemes d'informació	Conforme
14.2 Seguretat en els processos de desenvolupament i suport	Conforme
14.3 Les dades de prova	Conforme
15.1 Seguretat de la informació en relació amb els proveïdors	No Conforme
15.2 La gestió de la prestació de serveis de proveïdors	Conforme

16.1 Gestió dels incidents de seguretat de la informació i millores	No Conforme
17.1 La continuïtat seguretat de la informació	Conforme
17.2 Les redundàncies	Conforme
18.1 El compliment dels requisits legals i contractuals	Conforme
18.2 Opinions seguretat de la informació	Conforme



Per veure amb més detall l'auditoria, en l'ANNEX XIV podeu trobar l'informe d'auditoria pressuposant que hem implementat tots els projectes anteriorment definits.

Les millores observades respecte a la última revisió (2016) en cadascun dels controls auditats són:

Controls	Millores
5.1 Direcció de gestió de seguretat de la informació	Igual que anys anteriors
6.1 Organització interna	Igual que anys anteriors
6.2 Els dispositius mòbils i el teletreball	Igual que anys anteriors
7.1 Amb anterioritat a l'ocupació	Hi ha procediments per RRHH que proporcionen compliment de la Política de Seguretat relacionat amb els processos previs a la contractació.
7.2 Durant l'ocupació	Hi ha procediments per RRHH que proporcionen compliment de la Política de Seguretat relacionat amb els processos durant la durada del contracte.
7.3 Terminació i canvi d'ocupació	Hi ha procediments per RRHH que proporcionen compliment de la Política de Seguretat relacionat amb els processos en la finalització del contracte.

8.1 La responsabilitat dels actius	Els actius estan inventariats i s'han assignat a cada un dels responsables, s'han definit les normatives d'ús i devolució
8.2 Classificació de la Informació	La informació s'ha classificat i etiquetat en cadascuna de les àrees i s'han detallat procediments d'autorització i control d'accés segons la seva criticitat.
8.3 Mitjans de manipulació	Entre els actius gestionats es troben els suports d'emmagatzematge, amb un inventari de cada un d'ells, registre d'entrades i sortides.
9.1 Els requisits de negoci de control d'accés	Igual que anys anteriors
9.2 Gestió d'accés dels usuaris	Igual que anys anteriors
9.3 Responsabilitat dels usuaris	Igual que anys anteriors
9.4 Sistema de control i d'accés a les aplicacions	Igual que anys anteriors
10.1 controls criptogràfics	Igual que anys anteriors
11.1 Les àrees segures	Les sales i instal·lacions crítiques, on està ubicada la informació i els sistemes que la processen estan adequadament protegides contra accessos no autoritzats, amenaces ambientals i fallades de subministrament de serveis.
11.2 Equip	Igual que anys anteriors
12.1 Procediments i responsabilitats operacionals	En general els objectius de control definits per a aquest domini són realitzats de forma regular, es disposen de mecanismes per a la protecció contra programari maliciós i la gestió de la vulnerabilitat tècnica. Les còpies de seguretat són realitzades adequadament i els processos de recuperació estan provats amb regularitat.
12.2 Protecció contra el malware	
12.3 Còpia de seguretat	
12.4 Registre i supervisió	
12.5 de control de programari operacional	
12.6 La gestió tècnica de la vulnerabilitat	
12.7 Sistemes d'informació consideracions d'auditoria	
13.1 Gestió de seguretat de xarxa	Es verifica tant l'existència de mecanismes per garantir la seva seguretat (sistemes tallafocs, sistemes IDS / IPS o la segmentació de la xarxa), com la seva correcta implantació i configuració.
13.2 La transferència d'informació	Igual que anys anteriors
14.1 Els requisits de seguretat dels sistemes d'informació	Tots els sistemes i les URL publiques es troben darrera del WAF (web application firewall), tota la seguretat es gestiona a través de ells.
14.2 Seguretat en els processos de desenvolupament i suport	Es requeriment en els nous projecets la validació de Seguretat
14.3 Les dades de prova	Els entorns de preproducció i desenvolupament s'emmascaren les dades.
15.1 Seguretat de la informació en relació	Igual que anys anteriors

amb els proveïdors	
15.2 La gestió de la prestació de serveis de proveïdors	Des de l'àrea de RRHH es gestionen tota la documentació necessària abans de la prestació de servei, sense aquest requeriments l'empresa no té accés a les instal·lacions.
16.1 Gestió dels incidents de seguretat de la informació i millores	Igual que anys anteriors
17.1 La continuïtat seguretat de la informació	El Pla de Continuïtat de l'Organització, així com els Plans de Contingències estan definits i actualitzats adequadament. S'observen registres sobre les proves i verificacions de la seva eficàcia.
17.2 Les redundàncies	Es disposa d'un CPD de respatller amb els recursos físics i eines necessàries per restablir el servei dels processos crítics del negoci en el menor temps possible.
18.1 El compliment dels requisits legals i contractuals	Estan identificats els requeriments legals i reglamentaris que s'han de complir i s'han designats responsables de compliment encarregats d'assegurar el compliment.
18.2 Opinions seguretat de la informació	S'han establert processos que garanteixen la privacitat de les dades especialment protegides per la Llei de Protecció de Dades (LOPD) Es realitzen auditories regulars sobre el compliment normatiu i legal.

10. Conclusions

Durant el desenvolupament de tot aquest projecte s'ha establert les bases que permetran la implementació d'un Sistema de Gestió de la Seguretat de la Informació.

Els nivells de maduresa, tant del SGSI com el de l'Anàlisi de Riscos són inicials i requereixen evolucionar per acollir amb més detall els actius, els riscos i l'optimització de les mesures de seguretat existents o futures.

Els progressos aconseguits en la implantació del SGSI són:

- Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la Norma i fixar l'abast i objectius.
- Establir una base documental i determinar les responsabilitats de cada un dels components de l'estructura organitzativa de seguretat, de manera que s'asseguri la realització de totes les tasques necessàries i proporcionar Revisió i Millora.
- Identificar i inventariar els actius crítics de l'Organització, determinar la magnitud de les amenaces i, en darrer terme, concretar els riscos als que estan exposats els diferents elements dels Sistemes d'Informació de l'Organització.
- A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la Seguretat de l'Organització.

Aquest SGSI s'ha plantejat com un procés de millora contínua en constant actualització i renovació.

Inicialment es va realitzar una reducció dels actius, no inclouen la part de fàbrica, únicament IT, donat que el temps per a realitzar aquest Treball Final de Màster ha sigut uns 3 mesos, no arribàvem a les dates si analitzàvem tots els actius. Per tant, la planificació prevista ha sigut mitjanament adequada, donat que sempre s'ha complit amb les fases d'entrega.

En la nostra organització seguirem treballant donat que s'ha de realitzar un altra anàlisis de riscos amb els actius de fàbrica i les plantes de producció i em de tenir en compte altres tipus d'amenaces als que estem exposats.

11.Glossari

Definició dels termes i acrònims més rellevants utilitzats dins la Memòria.

Terme	Definició
SGSI	Sistemes de Gestió de la Seguretat de la Informació
AARR	Anàlisis de Riscos
Anàlisis de Riscos	El procés d'identificació dels riscos per a la seguretat del sistema i la determinació de la probabilitat d'ocurrència, l'impacte resultant, i les mesures de seguretat addicionals que mitiguin aquest impacte.
Mitigació de Riscos	Prioritzar, avaluar i implementar el risc adequada reducció dels controls / contramesures recomanades del procés de gestió de riscos.
Tolerància al risc	El nivell de risc que una entitat està disposat a assumir per tal d'aconseguir un resultat potencial desitjat
SCADA	Control de Supervisió i Adquisició de Dades.
Amenaça	Qualsevol circumstància o esdeveniment amb el potencial de tenir un impacte negatiu operacions de l'organització (incloent la missió, funcions, imatge o reputació), actius de l'organització, els individus, altres organitzacions o la nació a través d'un sistema d'informació a través d'un accés no autoritzat, destrucció, divulgació, modificació de la informació, i / o denegació de servei.
CSI	Comité de Seguretat de la Informació
RSI	Responsable de seguretat de la informació
CPD	Centres de processament de dades
ISO	International Organization for Standardization
CMDB	Base de Dades de la Gestió de Configuració
CMM	Model de Maduresa de la Capacitat

12. Bibliografia

1. Material MISTIC

Les referències bibliogràfiques utilitzades dins la memòria són referents als mòduls estudiats durant l'assignatura Sistemes de Gestió de la Seguretat:

- 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

Addicionalment s'ha consultat els següents mòduls de l'assignatura Auditoria:

- Mòdul 2. Auditoria de certificació ISO27001
- Mòdul 3. Auditoria tècnica de segureta

2. ISO/IEC 27000

ISO/IEC 27001:2013 - Requisits del Sistema de Gestió de Seguretat Informació.
ISO/IEC 27002:2013 - Objectius de control de la Norma ISO / IEC 27001
ISO_27000_implementation_guidance_v1_Spanish.pdf - www.iso27000.es Portal sobre la ISO 27001 en Español

13. Annexos

ANNEX I- Anàlisis diferencial ISO/IEC 27002:2013

Anàlisi diferencial en referència als objectius de control de la ISO/IEC 27002:2013. A continuació detallem el llistat amb els 114 controls i el corresponent CMM.

5. POLÍTIQUES DE LA SEGURETAT DE LA INFORMACIÓ	
5.1 Direcció de gestió de seguretat de la informació Objectiu: Proporcionar orientació i suport per a seguretat de la informació, d'acord amb els requeriments del negoci i les lleis i reglaments pertinents de gestió	
5.1.1 Les polítiques de seguretat de la informació	L5
5.1.2 Revisió de les polítiques de seguretat de la informació	L5
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ	
6.1 Organització interna Objectiu: Establir un marc de gestió per iniciar i controlar la implementació i operació de seguretat de la informació dins de l'organització.	
6.1.1 Rols i responsabilitats de seguretat de la informació	L4
6.1.2 La segregació de funcions	L3
6.1.3 Contacte amb les autoritats	L3
6.1.4 Contacte amb els grups d'interès especial	L3
6.1.5 Seguretat de la informació en la gestió de projectes	**L0**
6.2 Els dispositius mòbils i el teletreball Objectiu: Per garantir la seguretat del teletreball i l'ús de dispositius mòbils.	
6.2.1 política de dispositiu mòbil Una política de control	L0
6.2.2 El teletreball	L1
7. LA SEGURETAT DELS RECURSOS HUMANS	
7.1 Amb anterioritat a l'ocupació Objectiu: Garantir que els empleats i contractistes a entendre les seves responsabilitats i són adequats per a les funcions per a les que estan considerades.	
7.1.1 Control de Screening	L1
7.1.2 Termes i condicions d'ocupació	L3
7.2 Durant l'ocupació Objectiu: Garantir que els empleats i contractistes són conscients de les seves responsabilitats i compleixin seguretat de la informació	
7.2.1 Les responsabilitats de gestió	L4
7.2.2 Conscienciació sobre la seguretat de la informació, l'educació i la formació	L0
7.2.3 Procés disciplinari	L4
7.3 Terminació i canvi d'ocupació Objectiu: Per protegir els interessos de l'organització com a part del procés de canviar o acabar la feina.	
7.3.1 La terminació o el canvi de les responsabilitats d'ocupació	L1
8. GESTIÓ D'ACTIUS	

8.1 La responsabilitat dels actius Objectiu: Identificar els actius de l'organització i definir les responsabilitats de protecció adequats	
8.1.1 Inventari d'actius	L2
8.1.2 Propietat dels actius	L2
8.1.3 Ús acceptable dels actius	L3
8.1.4 Categories dels actius	L3
8.2 Classificació de la Informació Objectiu: Garantir que la informació rebi un nivell adequat de protecció d'acord amb la seva importància per a l'organització.	
8.2.1 Classificació de la informació	L0
8.2.2 Etiquetatge de la informació	L0
8.2.3 Manipulació dels procediments de control d'actius	L0
8.3 Mitjans de manipulació Objectiu: Per evitar la divulgació no autoritzada, modificació, eliminació o destrucció de la informació emmagatzemada en els mitjans de comunicació.	
8.3.1 Gestió de suports extraïbles	L2
8.3.2 Eliminació dels mitjans	L2
8.3.3 Transferència de mitjans físics	L2
9. CONTROL D'ACCÉS	
9.1 Els requisits de negoci de control d'accés Objectiu: Per limitar l'accés a les instal·lacions de processament d'informació i d'informació.	
9.1.1 Política de control d'accés	L3
9.1.2 L'accés a les xarxes i serveis de xarxa	L3
9.2 Gestió d'accés dels usuaris Objectiu: Garantir l'accés d'usuaris autoritzats i per evitar l'accés no autoritzat als sistemes i serveis	
9.2.1 Registre d'usuaris i baixes	L5
9.2.2 Accés aprovisionament d'usuaris	L5
9.2.3 Gestió de drets d'accés privilegiats	L2
9.2.4 Gestió de la informació de connexió de secret dels usuaris	L2
9.2.5 Revisió dels drets d'accés dels usuaris	L3
9.2.6 L'eliminació o ajust dels drets d'accés	L3
9.3 Responsabilitat dels usuaris Objectiu: fer que els usuaris responsables de salvaguardar la informació d'accés.	
9.3.1 Ús del control de la informació de connexió secreta	L2
9.4 Sistema de control i d'accés a les aplicacions Objectiu: Per prevenir l'accés no autoritzat a sistemes i aplicacions.	
9.4.1 Restricció d'accés a la informació	L3
9.4.2 Procediments de registre en-Secure	L3
9.4.3 Sistema de gestió de contrasenyes	L3
9.4.4 Ús dels programes de serveis públics privilegiats	L3
9.4.5 Control d'accés al codi font del programa	L3
10 Criptografia	

10.1 controls criptogràfics Objectiu: Per garantir l'ús adequat i eficaç de la criptografia per protegir la confidencialitat, autenticitat i / o integritat de la informació.	
10.1.1 Política sobre l'ús de controls criptogràfics	L0
10.1.2 Gestió de claus	L0
11 La seguretat física i ambiental	
11.1 Les àrees segures Objectiu: Prevenir l'accés no autoritzat física, dany i interferència a les instal·lacions de processament d'informació i la informació de l'organització.	
1.1.1 perímetre de seguretat física	L5
11.1.2 controls d'entrada físiques	L5
11.1.3 Protecció d'oficines, sales i instal·lacions	L3
11.1.4 Protecció contra amenaces externes i ambientals	L2
11.1.5 El treball en àrees segures	L4
11.1.6 Lliurament i càrrega de les zones	L4
11.2 Equip Objectiu: Per evitar la pèrdua, dany, robatori o el compromís dels actius i la interrupció de les operacions de l'organització.	
11.2.1 Emplaçament i la protecció de l'equip	L0
11.2.2 Suport als serveis públics	L5
11.2.3 La seguretat de cablejat	L3
11.2.4 El manteniment de l'equip	L3
11.2.5 Eliminació dels actius	L0
11.2.6 Seguretat dels equips i actius fora de l'establiment	L0
11.2.7 L'eliminació segura o la reutilització dels equips	L0
11.2.8 Equip d'usuari desatesa	L0
11.2.9 Esborrar escriptori i la política de pantalla transparent	L1
12 Operacions de Seguretat	
12.1 Procediments i responsabilitats operacionals Objectiu: Per garantir operacions correctes i segures d'instal·lacions de processament d'informació.	
12.1.1 procediments operacionals, adequadament documentats	L5
12.1.2 Gestió de canvis	L5
12.1.3 Capacitat de gestió	L5
12.1.4 Separació de desenvolupament, prova i entorns operatius	L5
12.2 Protecció contra el malware Objectiu: Garantir que les instal·lacions de processament d'informació i la informació estan protegits contra el malware.	
12.2.1 Controls contra el malware	L4
12.3 Còpia de seguretat Objectiu: Per evitar la pèrdua de dades.	
12.3.1 Informació de còpia de seguretat	L3
12.4 Registre i supervisió Objectiu: Per registrar els esdeveniments i generar evidència.	
12.4.1 registre d'esdeveniments	L5

12.4.2 Protecció de la informació de registre	L5
12.4.3 Administrador i operador registres	L5
12.4.4 Sincronització del rellotge	L5
12.5 de control de programari operacional Objectiu: Per garantir la integritat dels sistemes operatius.	
12.5.1 Instal·lació de programari en sistemes operatius	L5
12.6 La gestió tècnica de la vulnerabilitat Objectiu: Prevenir l'explotació de vulnerabilitats tècniques	
12.6.1 Gestió de vulnerabilitats tècniques	L5
12.6.2 Restriccions en la instal·lació del programari	L5
12.7 Sistemes d'informació consideracions d'auditoria Objectiu: Per minimitzar l'impacte de les activitats d'auditoria en els sistemes operatius.	
12.7.1 Sistemes d'informació controls d'auditoria	L2
13 Seguretat de les comunicacions	
13.1 de gestió de seguretat de xarxa Objectiu: Per garantir la protecció de la informació en xarxes i les seves instal·lacions de suport de processament d'informació.	
13.1.1 controls de xarxa	L4
13.1.2 Seguretat dels serveis de xarxa	L4
13.1.3 La segregació a les xarxes	L4
13.2 La transferència d'informació Objectiu: Per mantenir la seguretat de la informació transferida d'una organització i amb qualsevol	
13.2.1 polítiques i procediments de transferència d'informació	L4
13.2.2 Els acords sobre la transferència d'informació	L4
13.2.3 La missatgeria electrònica	L5
13.2.4 Confidencialitat o de no divulgació acords	L4
14 Sistema d'adquisició, desenvolupament i manteniment	
14.1 Els requisits de seguretat dels sistemes d'informació Objectiu: Garantir que la seguretat informàtica és una part integral dels sistemes d'informació a través de tot el cicle de vida. Això també inclou els requisits per als sistemes d'informació que proporcionen els serveis a través de xarxes públiques.	
14.1.1 Informació d'anàlisi de requisits de seguretat i les especificacions	L2
14.1.2 serveis d'aplicacions de fixació de les xarxes públiques	L2
14.1.3 Protecció de les transaccions de serveis d'aplicacions	L2
14.2 Seguretat en els processos de desenvolupament i suport Objectiu: Per assegurar que la seguretat d'informació es dissenya i implementa dins el cicle de vida de desenvolupament de sistemes d'informació.	
14.2.1 política de desenvolupament segur	L3
14.2.2 els procediments de control de canvis del Sistema	L3
14.2.3 Revisió tècnica d'aplicacions després de canvis en la plataforma d'operació	L3
14.2.4 Les restriccions als canvis en els paquets de programari	L3
14.2.5 principis d'enginyeria de sistemes segurs	L3

14.2.6 entorn de desenvolupament segur	L3
14.2.7 Desenvolupament externalitzat	L3
14.2.8 Les proves de seguretat del sistema	L3
14.2.9 Sistema de proves d'acceptació	L3
14.3 Les dades de prova Objectiu: garantir la protecció de dades que s'utilitza per a les proves	
14.3.1 Protecció de dades de prova	L0
15 Les relacions amb proveïdors	
15.1 Seguretat de la informació en relació amb els proveïdors Objectiu: Garantir la protecció dels actius de l'organització que sigui accessible pels proveïdors.	
15.1.1 La política de seguretat de la informació de relacions amb els proveïdors	L4
15.1.2 Abordar la seguretat dins dels acords amb proveïdors	L4
15.1.3 Cadena de la tecnologia d'informació i comunicació de subministrament	L4
15.2 La gestió de la prestació de serveis de proveïdors Objectiu: Mantenir un nivell acordat de seguretat de la informació i la prestació de serveis en línia amb els acords amb proveïdors.	
15.2.1 Seguiment i revisió dels serveis de proveïdors	L3
15.2.2 Gestió de canvis en els serveis de proveïdors	L3
16 Gestió d'incidents de seguretat d'informació	
16.1 Gestió dels incidents de seguretat de la informació i millores Objectiu: Per garantir un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, incloent-hi la comunicació d'esdeveniments i debilitats de seguretat.	
16.1.1 Responsabilitats i procediments	L0
16.1.2 Informes esdeveniments de seguretat de la informació	L0
16.1.3 Informes debilitats de seguretat d'informació	L0
16.1.4 L'avaluació i la decisió sobre els esdeveniments de seguretat d'informació	L0
16.1.5 Resposta a incidents de seguretat d'informació de control	L0
16.1.6 Aprenent dels incidents de seguretat de la informació	L0
16.1.7 Reunió de proves	L0
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	
17.1 La continuïtat seguretat de la informació Objectiu: la continuïtat seguretat de la informació ha de formar part dels sistemes de gestió de continuïtat de negoci de l'organització.	
17.1.1 Planificació de la continuïtat seguretat de la informació	L5
17.1.2 Implementació de la informació de seguretat de continuïtat	L5
17.1.3 Verificar, revisar i avaluar la informació de seguretat de continuïtat	L5
17.2 Les redundàncies Objectiu: assegurar la disponibilitat d'instal·lacions de processament d'informació.	
17.2.1 Disponibilitat d'instal·lacions de processament d'informació	L5
18 Compliment	
18.1 El compliment dels requisits legals i contractuals	

Objectiu: Per evitar l'incompliment de les obligacions legals, estatutàries, reglamentàries o contractuals relacionades amb la seguretat de la informació i de qualssevol requisits de seguretat.	
18.1.1 Identificació de la legislació aplicable i els requisits contractuals	L5
18.1.2 Drets de propietat intel·lectual	L5
18.1.3 Registres de control de registres	L5
18.1.4 Privacitat i protecció de dades personals	L5
18.1.5 Regulació de controls criptogràfics	L5
18.2 opinions seguretat de la informació Objectiu: Garantir que la seguretat informàtica és implementat i operat d'acord amb les polítiques i procediments de l'organització.	
18.2.1 Revisió independent de la seguretat de la informació	L5
18.2.2 El compliment de les polítiques i normes de seguretat	L5
18.2.3 Revisió de compliment tècnic	L5

ANNEX II- Política de Seguretat

POLÍTICA DE SEGURETAT

Data Publicació	Nom	Firma
08/03/2016	*Responsable de Seguretat*	TI Aprovació autor
10/03/2016	*Responsable de Riscos*	TI Aprovació revisor
17/03/2016	*Responsable de IT*	TI Aprovació

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis/Comentaris
01.00	17/03/2016	Responsable de Seguretat	Publicat	Versió Inicial

Índex

1. Objectiu 72
1.1. Sancions previstes per incompliment 73
2. Abast 73
3. Rols i responsabilitats 73
Comitè de direcció 73
Comitè de seguretat de la informació 74
Responsable de seguretat de la informació 74
Resta d'àrees 76
4. Compliment amb els requisits legals i estàndards de seguretat 76
5. Termes i definicions 76
6. Directrius de Seguretat 77
6.1. Directrius generals 77
6.2. Directrius sobre els sistemes informàtics laborals 78
6.3. Directrius sobre l'ús del correu electrònic 78
6.4. Directrius sobre l'ús de serveis en xarxa 79
6.5. Directrius sobre la propietat intel·lectual i industrial 79
6.6. Terceres empreses 79

1. Objectiu

Un dels principals objectius per la implantació d'un Sistema de Gestió de Seguretat de la Informació, en endavant SGSI, és el d'assentar unes bases sobre la seguretat dels nostres sistemes i poder gestionar els nostres productes, gestions bancàries, gestió de dades confidencials, etc. d'una manera segura.

Política de Seguretat garanteix la continuïtat dels sistemes de la informació, minimitzar els riscs de danys, assegurar l'eficient compliment dels objectius de Traun i garantir l'aplicació de la legislació actual referent al tractament de dades i sistemes de la informació.

La gestió de la seguretat de la informació ha de garantir el funcionament adequat de les activitats de control, monitorització i manteniment de les infraestructures e instal·lacions.

En l'avaluació dels controls generals de TI, el sistema cobreix els següents processos:

- Gestió d'identitats i autoritzacions d'accés;
- Desenvolupament i implantació de nous projectes;
- Canvis evolutius i correctius;
- Control ambiental i accés físic als centres de procés de dades;
- Salvaguarda de la informació, plans de recuperació i continuïtat.
- Operació i monitoratge dels sistemes i aplicacions;
- Gestió d'incidències; Les debilitats detectades, quan no s'identifiquen controls compensatoris que les mitiguen, són esmenades mitjançant plans de remediació específics. Així mateix, per a la seguretat de la informació, la Societat disposa d'una sèrie de polítiques i procediments que estableixen i defineixen, entre altres, els següents principis de funcionament:
- Metodologia de desenvolupament: cobrint des de la presa de requeriments fins al testing i acceptació per part de la unitat de negoci té com a objectiu principal assegurar que els sistemes es comporten segons s'han definit;
- Fluxos de revisió i aprovació de les especificacions i documentació de disseny d'aplicacions, canvis a programes i sistemes, així com de l'assignació dels accessos a la informació;
- Monitorització de la disponibilitat de sistemes i aplicacions així com de la integritat de les dades intercanviades entre les aplicacions rellevants;
- Segregació de funcions basada en una matriu d'incompatibilitats, supervisada pels responsables dels diferents processos de negoci;
- Pla de recuperació en ubicació secundària dels sistemes rellevants;
- Política d'ús dels sistemes d'informació. La gestió de la seguretat de la informació i actius tecnològics associats, així com la responsabilitat, en l'àmbit

dels processos TI, sobre el compliment normatiu i el manteniment de privacitat de les dades de clients, empleats, i donants recau sobre els següents òrgans :

- Comitè de seguretat de TI: Analitza periòdicament els diferents informes de riscos, incidents i canvis normatius i proposa els plans d'acció que considera adequats per protegir els actius d'informació i per assolir i mantenir el nivell de seguretat desitjat;
- Funció de Gestió del Risc TI: Depenent directament del director de TI, té com a principal missió analitzar els riscos dels diferents processos, sistemes i aplicacions i mantenir-los en uns nivells acceptats per la societat, desenvolupant i coordinant la implantació dels controls, en cas necessari.

1.1. Sancions previstes per incompliment

L' incompliment de les disposicions establertes per les Polítiques de Seguretat de la Informació tindrà com a resultat l'aplicació de diverses sancions, d'acord amb la magnitud i característica de l'aspecte no complert.

2. Abast

L'abast d'aquesta política es per a tot el personal de la plantilla Traun, així com les persones que es trobin donant servei i que tinguin accés a actius de la informació.

En aquesta política s'engloba tots els actius de la informació que l'empresa disposa a dia d'avui, entre ells estan les dades, els recursos tecnològics, els locals i les persones que els accedeixen d'alguna manera.

3. Rols i responsabilitats

Comitè de direcció

Les funcions en matèria de seguretat de la informació del comitè de direcció de la companyia són les següents:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres d'un comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar riscos possibles introduïts per canvis en les funcions o en el funcionament de la companyia per a adoptar les mesures de seguretat més adequades.
- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en la matèria.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

Les decisions preses pel comitè de direcció en matèria de seguretat de la informació han de quedar recollides en acta.

Comitè de seguretat de la informació
Les decisions en matèria de seguretat de la informació les pren de manera consensuada un grup format per diferents responsables dins de la companyia.

Les funcions en matèria de seguretat de la informació del comitè de seguretat de la informació són les següents:

- Implantar les directrius del comitè de direcció.
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.
- Validar el mapa de riscos i les accions de mitigació que ha proposat el responsable de seguretat de la informació.
- Validar el pla de seguretat de la informació o pla director de seguretat de la informació i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.
- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.
- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.
- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.
- Revisar les incidències més destacades.
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució de l'SGSI.

Responsable de seguretat de la informació
La designació d'un responsable de seguretat de la informació (RSI) és l'única via per a avançar de manera organitzada i gradual en seguretat de la informació, ja que garanteix que hi ha algú per a qui la seguretat de la informació és una prioritat.

Les funcions en matèria de seguretat de la informació dels RSI són coordinar les accions orientades a garantir la seguretat de la informació en qualsevol de les formes que té (digital, òptica, paper, etc.) i en tot el cicle de vida d'aquesta informació (creació, manteniment, distribució, emmagatzematge i destrucció), per a protegir-la en termes de confidencialitat, privadesa, integritat, disponibilitat, autenticitat i traçabilitat.

Tot plegat es concreta en els punts següents:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius en matèria de seguretat de la informació.

- Desenvolupar i mantenir el document d'Organització de la seguretat de la informació en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les responsabilitats en seguretat i també una descripció detallada de funcions i dependències.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.
- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.
- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

Responsable de riscos

- Vetllar pel compliment legal (LOPD, RD 3/2010, Esquema nacional de seguretat, Basilea, SOX, etc.) i coordinar les actuacions necessàries amb les unitats responsables.
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.

- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).

Resta d'àrees
Cada àrea dins de la companyia ha de col·laborar amb l'RSI a desplegar la seguretat en el seu àmbit d'actuació i a aconseguir treballar i fer treballar l'organització de manera segura. Així, doncs, també s'han d'identificar funcions de seguretat en els àmbits d'auditoria, assegurances, formació, organització, etc.

4. Compliment amb els requisits legals i estàndards de seguretat

Es pren com a referència, sense caràcter exhaustiu, la següent legislació:

- Llei 7/1985, del 2 d'abril, Reguladora de les Bases del Règim Local.
- Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal i les seves normes de desenvolupament.
- Llei 34/2002, de l'11 de juliol, de serveis de la societat de la informació i del comerç electrònic.
- Llei 32/2003, del 3 de novembre, General de Telecomunicacions.
- Llei 59/2003, del 19 de novembre, de signatura electrònica.
- Real Decret 1720/2007, del 21 de desembre, pel qual s'aprovà el Reglament de desenvolupament de la Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal
- COBIT 5: Objectius de Control per a la Informació i Tecnologies Relacionades
- Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la Llei de Propietat Intel·lectual (LPI), regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria
- ISO / IEC 27001: 2013 Tecnologia de la informació - Tècniques de seguretat - Sistemes de gestió de seguretat de la informació - Requisits ISO / IEC 27002: 2013 Tecnologia de la informació - Tècniques de seguretat - Codi de pràctiques per als controls de seguretat de la informació.

5. Termes i definicions

Terme	Definició
Confidencialitat	Es garanteix que la informació sigui accessible només a aquelles persones autoritzades a tenir accés a la mateixa.
Integritat	Es salvaguarda l'exactitud i totalitat de la informació i els mètodes de processament.

Disponibilitat	Es garanteix que els usuaris autoritzats tinguin accés a la informació i als recursos relacionats amb la mateixa, tota vegada que el requereixin.
Autenticitat	Busca assegurar la validesa de la informació en temps, forma i distribució. Així mateix, es garanteix l'origen de la informació, validant l'emissor per evitar suplantació d'identitats.
Auditabilitat	Defineix que tots els esdeveniments d'un sistema han de poder ser registrats per al seu control posterior.
Informació	Es refereix a tota comunicació o representació de coneixement com dades, en qualsevol forma, amb inclusió de formes textuals, numèriques, gràfiques, cartogràfiques, narratives o audiovisuals, i en qualsevol mitjà, ja sigui magnètic, en paper, en pantalles d'ordinadors, audiovisual o un altre.
Sistema d'Informació	Es refereix a un conjunt independent de recursos d'informació organitzats per a la recopilació, processament, manteniment, transmissió i difusió d'informació segons determinats procediments, tant automatitzats com manuals.
Tecnologia de la Informació	Es refereix al maquinari i programari operats pel Organisme o per un tercer que processi informació en el seu nom, per dur a terme una funció pròpia, sense tenir en compte la tecnologia utilitzada, ja es tracti de computació de dades, telecomunicacions o un altre tipus.
Comitè de Seguretat de la Informació	El Comitè de Seguretat de la Informació, és un cos integrat per representants de totes les àrees substantives de l'Organisme, destinat a garantir el suport manifest de les autoritats a les iniciatives de seguretat.
Responsable de Seguretat Informàtica	És la persona que compleix la funció de supervisar el compliment de la present Política i d'assessorar en matèria de seguretat de la informació als integrants de l'Organisme que així ho requereixin.

6. Directrius de Seguretat

Es l'obligació de tot el personal de Traun, així com les persones que prestin serveis temporalment el conèixer els següents apartats:

6.1. Directrius generals

- El sistema informàtic, la xarxa corporativa i els dispositius mòbils utilitzats per cada usuari, són propietat de Traun, proporcionats únicament per la prestació laboral i en cap cas per les activitats personals.
- L'empresa es reserva el dret de fiscalitzar l'ús dels equips informàtics i d'accedir a la informació emmagatzemada o transmesa utilitzant els sistemes informàtics propietat de l'empresa, amb el propòsit d'auditar i comprovar que el seu ús s'ajusta a les finalitats que els justifiquen i poder detectar i / o prevenir violacions de seguretat.
- Únicament podran accedir als fitxers i dades per als que compti amb accés autoritzat i fer ús de la informació allà continguda només si és necessari per a

desenvolupar la tasca professional que tenen encomanada. Si per error pogués accedir a dades protegides no autoritzats ho comunicarà urgentment al responsable de seguretat.

- No poden traslladar els fitxers i les dades fora dels centres de treball de Traun mitjançant cap tipus de suport, llevat que obtinguin l'autorització expressa i amb les mesures de seguretat adequades.
- Tots els procediments i activitats realitzades amb els sistemes de la informació han d'utilitzar mecanismes que permetin identificar inequívocament l'usuari que el realitza. Així com emmagatzemar registres d'aquesta activitat per disposar de la traçabilitat.
- El Identificador i la clau d'accés és personal i intransferible, sent el seu propietari l'únic responsable. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i accés haurà activar els mecanismes de sol·licitud de canvi de contrasenya e informar com una incidència.
- És responsabilitat de Traun proporcionar i revocar els privilegis d'accés a la informació i les tecnologies que la suporten.
- S'aplicaran mesures tecnològiques per garantir la seguretat de les claus d'accés i que assegurin un nivell de robustesa adequat.

6.2. Directrius sobre els sistemes informàtics laborals

- Tot fitxer temporal o còpia de treball amb dades personals creat exclusivament per a la realització de treballs temporals serà esborrat o destruït una vegada que hagi deixat de ser necessari per als fins que van motivar la seva creació.
- L'usuari no ha de emmagatzemar dades de caràcter personal en el disc dur de l'ordinador.
- S'aplicaran mesures tecnològiques necessàries per garantir la seguretat dels equips desatesos.
- Els usuaris observessin les mesures de seguretat establertes quan s'absentin del lloc de treball, activat l'estalvi de pantalla o bloquejant l'equip.
- Es recomana apagar l'equip en finalitzar la jornada laboral, sempre que sigui possible, per facilitar la incorporació d'actualitzacions i millorar el seu manteniment.

6.3. Directrius sobre l'ús del correu electrònic

- Cap missatge de correu electrònic utilitzant els mitjans informàtics proporcionats per Traun serà considerat com privat. Es considera correu electrònic tant l'intern, entre terminals de la xarxa corporativa, com l'extern, dirigit o provinent d'altres xarxes privades o públiques, especialment Internet.
- Tal com es ve establint en el present document, la utilització del correu electrònic en els termes descrits en el paràgraf anterior ha exclusivament em per una utilització laboral o professional.
- No enviarà missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitàries sense el consentiment del destinatari.
- No enviarà o reenviarà missatges en cadena o de tipus piramidal.

- Qualsevol fitxer introduït en la xarxa corporativa o al terminal de l'usuari a través de missatges de correu electrònic, provinents de xarxes externes, ha de complir els requisits establerts en aquestes normes, especialment, les referides a propietat intel·lectual i industrial i a control de virus.

6.4. Directrius sobre l'ús de serveis en xarxa

- L'ús del sistema informàtic de Traun per accedir a xarxes públiques com Internet, quan hi hagi l'autorització de l'Organització, es limitarà als temes directament relacionats amb l'activitat i les comeses del lloc de treball de l'usuari.
- Els serveis de missatgeria instantània i xats així com xarxes socials no estan autoritzats, amb l'excepció d'aquells que siguin requerits per al desenvolupament de les funcions del seu lloc de treball.
- Els Serveis punt a punt o descàrregues directes, són especialment perillosos, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, pel que el seu ús queda estrictament prohibit.
- L'accés, en cas de ser autoritzat per Traun, a pàgines web, grups de notícies i altres fonts d'informació, es limita a aquells que continguin informació relacionada amb l'activitat o amb les comeses del lloc de treball de l'usuari.
- Qualsevol fitxer introduït en la xarxa corporativa o al terminal de l'usuari des d'Internet, quan hagués estat autoritzat per Traun, ha de complir els requisits fixats en l'autorització i en aquestes normes i, especialment, les referides a propietat intel·lectual i control de virus .
- S'aplicarà a l'accés i ús d'Internet les mateixes regles i exigències establertes per a l'ús del correu electrònic, en relació amb els principis que regeixen l'accés i ús, i informació prèvia sobre possibilitat de control amb vista a comprovar la correcció dels usos.

6.5. Directrius sobre la propietat intel·lectual i industrial

Queda estrictament prohibit l'ús de programes informàtics sense la corresponent llicència, així com l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial.

6.6. Terceres empreses

Si Traun requereix de serveis de tercers. Aquest tercer haurà d'acceptar les obligacions establertes en la normativa. S'establiran procediments específics d'informació i notificació d'incidències.

Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix en el paràgraf anterior, es requerirà un informe del Responsable de Riscos que presenti els riscos en que s'incorre i la forma de tractar-los, si és possible. Es requerirà llavors de l'aprovació d'aquest informe per part dels responsables de la informació.

ANNEX III- Procediment d'auditoria interna

PROCEDIMENT D'AUDITORIA TRAUN

Data Publicació	Nom	Firma
21/03/2016	*Responsable de Seguretat*	TI Aprovació autor
04/04/2016	*Responsable de Riscos*	TI Aprovació revisor
06/04/2016	*Responsable de IT*	TI Aprovació

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis/Comentaris
01.00	Pendent	Responsable de Seguretat	Publicat	Versió Inicial

Índex

1. Introducció 82
2. Objectiu 82
3. Abast 82
4. Procediment 82
4.1.1. Planejament i programació 82
4.1.2. Execució de l'Auditoria 83
4.1.3. Informe i Pla d'Acció 83
5. Resultats 83
6. Seguiment de l'auditoria i finalització 83

1. Introducció

Per verificar que els controls, processos i procediments del Sistema de Gestió de Seguretat de la Informació segueix conforme la norma i la legislació vigent, així com validar que els objectius de seguretat de l'organització estan implementats, mantinguts amb eficàcia i tenen el rendiment esperat, que es duen a terme contractant auditors externs.

Els auditors han de complir els requisits següents:

- Han de ser independents, és a dir, no poden haver intervingut en el procés o treball auditat.
- Han d'estar qualificats en la matèria: coneixement del procés d'auditoria i de les normes auditades i, si pot ser, han de tenir experiència en el camp de la seguretat de la informació.
  Aquestes auditories s'han de planificar correctament, perquè hi estiguin implicades totes les persones necessàries.

2. Objectiu

L'objectiu d'aquest procediment es especificar els requeriments i processos que han de realitzar-se juntament amb els encarregats de realitzar-les, per establir un pla d'auditoria de seguretat de la informació.

La realització periòdica d'aquest d'auditories, serveixen per assegurar que l'organització segueix operant en el marc de les polítiques, procediments i requeriments externs establerts per tal de garantir els objectius de Traun.

3. Abast

L' abast d'aquest procediment d'auditoria és el mateix que hi ha definit en l'abast del SGSI.

4. Procediment

La pràctica de l'Auditoria es divideix en tres fases:

1. Plantejament i programació
2. Execució de l'Auditoria
3. Informe i Pla d'Acció

4.1.1. Planejament i programació

En aquesta fase s'estableixen les relacions entre auditors i l'entitat, és el coneixement global de l'empresa per part de l'auditor en on es determina l'abast i objectius. Es fa un esbós de la situació de l'entitat, sobre la seva organització, sistema comptable, controls interns, estratègies, metodologies i altres elements que li permetin a l'auditor elaborar el programa d'auditoria que es durà a efecte.

4.1.2. Execució de l'Auditoria

L'objectiu d'aquesta etapa és obtenir i analitzar tota la informació del procés que s'audita, amb la finalitat d'obtenir evidència suficient, competent i rellevant, és a dir, comptar amb tots els elements que li assegurin a l'auditor l'establiment de conclusions fundades en el informe sobre les situacions analitzades en terreny, que entre altres incloguin: el nivell efectiu d'exposició al risc; les causes que l'originen; els efectes o impactes que es podrien ocasionar a materialitzar un risc i, basant-se aquestes anàlisis, generar i fonamentar les recomanacions que hauria d'acollir l'Administració.

4.1.3. Informe i Pla d'Acció

És el resultat de la informació, estudis, investigació i anàlisis efectuades pels auditors durant la realització d'una auditoria, que de forma normalitzada expressa per escrit la seva opinió sobre l'àrea o activitat auditada en relació amb els objectius fixats, assenyalen les debilitats de control intern, si n'hi ha hagut, i formula recomanacions pertinents per eliminar les causes de tals deficiències i establir les mesures correctores adients.

5. Resultats

L'informe d'auditoria ha d'incloure la següent informació:

- Data de l'auditoria.
- Nom dels auditors.
- Abast de l'auditoria: àrea, departament i/o processos auditats.
- Controls auditats.
- Conformitat de l'SGSI amb la norma, o grau d'adequació.
- No-conformitats detectades.
- Si l'auditoria no és de certificació, pot contenir, a més, recomanacions de millora.

6. Seguiment de l'auditoria i finalització

L'equip d'auditoria es responsable d'identificar les diferents no conformitats.
L'organització és la responsable de resoldre les no conformitats reportades.

Les accions correctives seran planificades o previstes en comú acord entre el Comitè De Seguretat de la Informació i l'equip d'auditors.

L'auditoria es considerarà finalitzada un cop reportat les no conformitats.
L'organització disposarà de 3 mesos per corregir les mesures correctives.

A continuació es detalla l'estructura de plantilla de les no conformitats:

Àrea	**Descripció de l àrea**	Conclusió	(1)

Control ISO: Nombre
Descripció del control de la ISO/IEC 27002:2013

Treball realitzat
És detalla la feina realitzada en aquesta area concreta.

Observació
És detalla els possibles aspectes destacats així com observacions relacionades amb l'àrea.

Evidencies
És detallen les evidencies recollides, les quals donen suport al treball realitzat i les observacions efectuades utilitzant la següent nomenclatura **EV_XXX**, on: ▪ **EV** es la abreviatura de l'evidencia ▪ **XXX** és el número de l'evidencia dintre l'informe

Recomanació
S'adjunta les recomanacions sobre les observacions del punt anterior.

Estat	(2)	Responsable	(3)	Termini	(4)

(1): Conforme (fons verd) / No Conforme (fons vermell) / No aplica
(2): Pendent / En curs / -- (en caso de no haver recomanacions)
(3): Area o persona responsable / -- (en caso de no haver recomanacions)
(4): 1 mes / 3 meses / 6 meses / + de 6 meses / -- (en caso de no haver recomanacions)

ANNEX IV- Procediment d'anàlisis i gestió de riscos

PROCEDIMENT D'ANÀLISIS I GESTIÓ DE RISCOS

Data Publicació	Nom	Firma
08/03/2016	*Responsable de Riscos*	TI Aprovació autor
08/03/2016	*Responsable de Seguretat*	TI Aprovació revisor
16/03/2016	*Responsable de IT*	TI Aprovació

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis/Comentaris
01.00	16/03/2016	Responsable de Riscos	Publicat	Versió Inicial

Índex

1. Objectiu 87
2. Abast 87
3. Rols i responsabilitats 87
4. Termes i definicions 87
5. Metodologia d'anàlisis de riscos 88
6. Fases de Magerit 88
6.1. Presa de dades i processos d'informació 88
6.2. Dimensionament, Establiment de paràmetres 88
6.3. Anàlisis d'actius 90
6.4. Anàlisis d'amenaces 90
6.5. Establiment de Vulnerabilitats 91
6.6. Establiment d'impactes 91
6.7. Anàlisi de risc intrínsec 91
6.8. Influència de controls de Seguretat 91
6.9. Anàlisi de riscos efectiu 91
6.10. Avaluació de riscos 92

1. Objectiu

L'objectiu del procediment es establir la metodologia i activitats per realitzar l'Anàlisi i gestió de riscos de Traun.

Aquest procediment permet identificar els riscos a què està exposada l'organització, permet a l'organització fer una selecció de les mesures de seguretat que s'hi han d'implantar, molt més ajustada a les necessitats d'aquesta organització, permet fer i elaborar els plans de contingències d'una organització.

2. Abast

L' abast d'aquest procediment d'auditoria és el mateix que hi ha definit en l'abast del SGSI.

3. Rols i responsabilitats

Tasca \ Owner	Responsable Risc	Responsable Seguretat	Responsable TI
Elaboració i revisió de l'Anàlisis de Riscos	R	I/C	A
Gestió del Risc	R	I/C	A
Actualització i seguiment del Pla de Riscos	R	I/C	A
Elaboració del Pla d'implementació dels Controls.	R	I/C	A

4. Termes i definicions

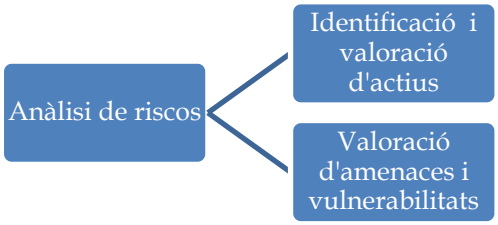
Terme	Definició
Confidencialitat	Es garanteix que la informació sigui accessible només a aquelles persones autoritzades a tenir accés a la mateixa.
Integritat	Es salvaguarda l'exactitud i totalitat de la informació i els mètodes de processament.
Disponibilitat	Es garanteix que els usuaris autoritzats tinguin accés a la informació i als recursos relacionats amb la mateixa, tota vegada que el requereixin.
Actius	Elements que s'han de protegir
Amenaces	Situacions de què s'han de protegir els actius
Vulnerabilitats	Aspectes que faciliten la materialització de les amenaces
Cost de protecció	Cost que comporta a l'organització protegir-se d'una situació detectada prèviament
Cost d'exposició	Cost que representaria que s'arribés a donar la situació analitzada i l'organització no tingués protecció
Impactes	Les conseqüències que es produeixen en l'organització quan una amenaça aprofita una vulnerabilitat per a danyar un actiu

Risc Intrínsec	Els riscos a què estem exposats sense tenir en compte les mesures de seguretat que implantem.

5. Metodologia d'anàlisis de riscos

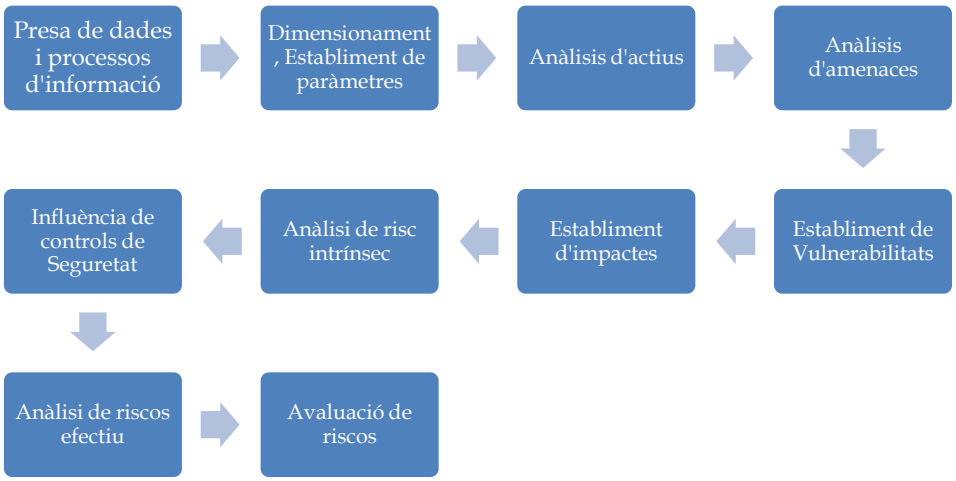
La metodologia aplicada en Traun serà la de Magerit.

El risc consisteix en la relació d'aquests tres elements. Combinant-los entre si s'obté els diferents tipus de riscos a què està exposada una organització:



6. Fases de Magerit

Magerit segueix un procés fins a arribar a elaborar i identificar tots els riscos d'una organització. Les fases són les següents:



6.1. Presa de dades i processos d'informació

En aquesta fase s'ha de definir l'abast de l'anàlisi de riscos, s'han d'analitzar els processos que duu a terme l'organització, ja que els riscos que s'estudiaran són els que poden interferir en els processos crítics.

6.2. Dimensionament, Establiment de paràmetres

Un cop realitzada la presa de dades, s'estableix els paràmetres que s'utilitzaran durant tot el procés d'anàlisi de riscos.

Els paràmetres que s'identifiquen en aquesta fase, permeten quantificar els diferents elements utilitzats en l'anàlisi de riscos, es important utilitzar els mateixos paràmetres en tot el procés.

Els paràmetres que s'han d'identificar són els següents:

- **Valor dels actius**, l'objectiu d'assignar una valoració econòmica a tots els actius d'una organització que es pretenen analitzar.
- **Vulnerabilitat**, s'entenen com una freqüència d'ocurrència d'una amenaça.
  Vulnerabilitat = freqüència estimada / dies de l'any
- **Impacte**, tant per cent del valor de l'actiu que es perd en cas que hi hagi una incidència sobre aquest actiu
- **Efectivitat del control de seguretat,** consisteix a veure la influència que tindran les mesures de protecció davant els riscos que detectem, és a dir, a pensar en la manera com ens poden reduir el risc detectat les diferents mesures de seguretat que implantem.

Valoració d'actius		
Descripció	Abreviatura	Valor
Molt alt	DT.	300.000
Alt	A	150.000
Mitjà	M	75.000
Baix	B	30.000
Molt baix	MB	10.000
Menyspreable	D	5.000

Freqüència		
Descripció	Abreviatura	Valor
Extremadament freqüent	EF	1
Molt freqüent	MF	0,07123288
Freqüent	F	0,01643836
Poc Freqüent	PF	0,0109589
Molt poc freqüent	MPF	0,00547945
Menyspreable	D	0,00273973
Dies:	365	

Impacte		
Descripció	Abreviatura	Valor
Critico	C	90%
Alt	A	75%

Mitjà	M	50%
Baix	B	20%

6.3. Anàlisis d'actius

En aquesta fase s'han d'identificar tots els actius disponibles en l'organització i que es troben dins de l'abast, de tal manera que els podem classificar en funció dels valors establerts prèviament.

Es considera actiu dels sistemes de la informació la següent agrupació:

• Actius físics. Són tots els actius de tipus hardware.

• Actius lògics. Són tots els actius de tipus software.

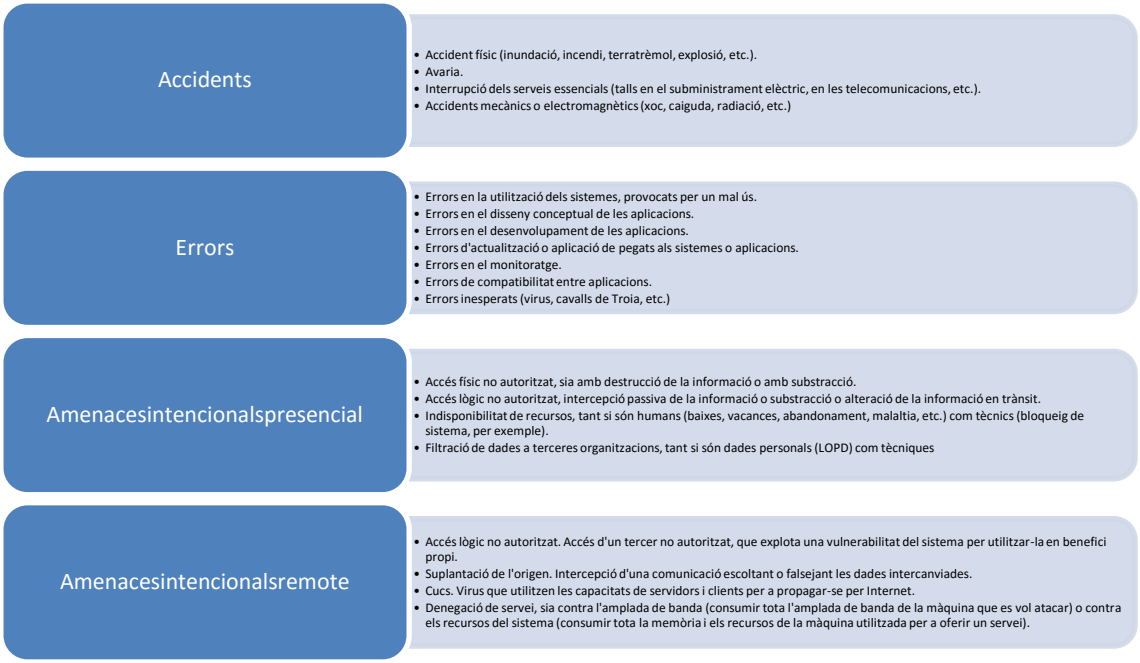
• Actius de personal. Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització.

• Actius intangibles. Són els elements que no té directament l'organització però que són importants per a ella.

6.4. Anàlisis d'amenaces

Un cop hem identificat els actius, procedim a analitzar les amenaces que poden afectar-les tenint en compte que cada organització té una casuística concreta.

Magerit classifica les amenaces que poden afectar una organització en quatre grans grups, i dins de cadascun d'aquests grups identifica amenaces més concretes, que són les que s'han de preveure:



6.5. Establiment de Vulnerabilitats

En Magerit, malgrat que no és necessari fer una llista de les vulnerabilitats, sí que ho és tenir-les en compte per a estimar la freqüència d'ocurrència d'una determinada amenaça sobre un actiu.

6.6. Establiment d'impactes

En aquesta fase es realitza les valoracions del impacte que pot provocar en l'empresa les amenaces existents, s'ha d'analitzar:

- El resultat de l'agressió d'una amenaça sobre un actiu.
- L'efecte sobre cada actiu per a agrupar els impactes en cadena segons la relació d'actius.
- El valor econòmic representatiu de les pèrdues produïdes en cada actiu.
- Les pèrdues quantitatives o qualitatives.

6.7. Anàlisi de risc intrínsec

Amb les dades obtingudes en fases anteriors, es pot calcular el Risc Intrínsec, es a dir, l'anàlisi de la situació en què es troba l'organització en el moment de l'estudi encara que ja tingui implantades mesures de seguretat.

$$\textbf{\textit{Risc}} = \textit{Valor de l'actiu} \times \textit{Vulnerabilitat} \times \textit{Impacte}$$

6.8. Influència de controls de Seguretat

En aquesta fase, la fase de gestió de riscos, que consisteix a mirar d'escollir la millor solució de seguretat que ens permeti reduir-los. Hi ha dos tipus fonamentals de controls de seguretat:

• Preventius. Són les mesures de seguretat que redueixen les vulnerabilitats (la freqüència d'ocurrència).

• Correctius. Són les mesures de seguretat que redueixen l'impacte de les amenaces.

6.9. Anàlisi de riscos efectiu

En aquesta fase veurem com es reduiran els riscos aplicant les mesures de seguretat que s'han determinat anteriorment. D'aquesta manera podrem realitzar una aproximació del risc efectiu.

$$\textbf{\textit{Risc Efectiu}} = \textit{Valor efectiu} \times \textit{Nova vulnerabilitat} \times \textit{Nou impacte} = \textit{Valor actiu} \times (\textit{Vulnerabilitat} \times \textit{Percentatge de disminució de vulnerabilitat}) \times (\textit{Impacte} \times \textit{Percentatge de}$$

disminució d'impacte) = Risc intrínsec × Percentatge de disminució de vulnerabilitat × Percentatge de disminució d'impacte

6.10. Avaluació de riscos

Aquesta última fase consisteix en la presa de decisions de l'organització sobre les mesures de seguretat que ha d'escollir entre la llista de controls de seguretat que li permeten reduir els riscos.

A l'hora de gestionar riscos s'ha d'elaborar un plad'acció, que ha de contenir la informació següent:

• Establir prioritats. Consisteix a designar els riscos que s'han de reduir en primer lloc perquè són els més elevats per a l'organització.

• Plantejar l'anàlisi de cost-benefici. Consisteix a estudiar, per a cadascuna de les mesures que es poden implantar, quin cost comporta a l'organització i en quin percentatge redueix els riscos detectats.

• Seleccionar controls definitius. Una vegada analitzat el cost-benefici de tots els controls, cal seleccionar definitivament els que ha d'implantar l'organització per a reduir els riscos fins a situar-los per sota del seu llindar de risc.

• Assignar responsabilitats. Consisteix a assignar els responsables dins de l'organització de dur a terme la implantació dels controls. És important tenir identificades aquestes persones ja que, si no, hi ha el perill que les decisions que es prenguin no s'acabin implantant.

• Implantar controls. Consisteix a implantar els controls de seguretat designats. Cal tenir en compte que els controls que s'implanten no han de ser forçosament tècnics, sinó que poden ser controls organitzatius o procedimentals.

ANNEX V- Gestió d'indicadors de Seguretat

A continuació detallem cada un dels indicadors ja implementats en Traun, seguint els vuit components bàsics:

Control de l'ISO amb què està relacionat	
5. Polítiques de la Seguretat de la Informació	
Objectiu de l'indicador	**Definició**
Busca identificar el nivell d'estructuració dels processos de l'entitat orientats a la seguretat de la informació.	Compliment de polítiques de seguretat de la informació en l'entitat
Responsable de la mesura	**Freqüència**
Responsable de Seguretat	Anual
Fórmula de mesurament	**Descripció dels valors**
SI.5 = 1 (SI s'evidencia) SI.5 = 0 (NO s'evidencia)	L'entitat ha definit una política general de seguretat de la informació? L'entitat ha definit una organització interna en termes de persones i responsabilitats per tal de complir les polítiques de seguretat de la informació i documenta aquestes activitats? L'entitat compleix amb els requisits legals, reglamentaris i contractuals respecte al maneig de la informació?
Valor objectiu de l'indicador	
1	

Control de l'ISO amb què està relacionat	
18 Compliment	
Objectiu de l'indicador	**Definició**
Busca identificar l'existència de directrius, normes o estàndards quant registre i auditoria per a la seguretat de la informació.	Grau d'existència de directrius, normes o estàndards quant registre i auditoria per a la seguretat de la informació.
Responsable de la mesura	**Freqüència**
Responsable de Seguretat	Anual
Fórmula de mesurament	**Descripció dels valors**

SI.18 = 1 (SI s'evidencia) SI.18 = 0 (NO s'evidencia)	L'entitat ha definit directrius, normes i / o estàndards per al registre i control d'esdeveniments que succeeixin sobre els seus sistemes, xarxes i serveis? L'entitat verifica de manera interna i / o mitjançant tercers, periòdicament els seus processos de seguretat de la informació i sistemes per assegurar el compliment del model?
Valor objectiu de l'indicador	
1	

Control de l'ISO amb què està relacionat	
6. Organització de la Seguretat de la Informació	
Objectiu de l'indicador	**Definició**
Fer un seguiment a l'assignació de recursos i responsabilitats en gestio de seguretat de la informació, per part de l'alta direcció.	L'indicador permet determinar i fer seguiment, al compromís de la direcció, quant a seguretat de la informació, pel que fa a la assignació de persones i responsabilitats relacionades a la seguretat de la informació a l'interior de l'entitat
Responsable de la mesura	**Freqüència**
Responsable de Seguretat	Anual
Fórmula de mesurament	**Descripció dels valors**
S.6=(SI61/SI62)*100	SI61.Número de personas con su respectivo rol SI62.Nombre de persones amb el seu respectiu paper va definir després d'un any
Valor objectiu de l'indicador	
80%	

Control de l'ISO amb què està relacionat	
9. Control d'accés	
Objectiu de l'indicador	**Definició**
Busca identificar l'existència de directrius, normes o estàndards pel que fa al control d'accés a l'entitat.	Grau control d'accés a l'entitat.
Responsable de la mesura	**Freqüència**

Responsable de Seguretat	Anual
Fórmula de mesurament	**Descripció dels valors**
SI.9 = 1 (SI s'evidencia) SI.9 = 0 (NO s'evidencia)	L'entitat ha definit directrius, normes i / o estàndards per controlar l'accés dels usuaris als seus serveis de Govern en línia i a les seves xarxes de comunicacions? L'entitat ha definit directrius, normes i / o estàndards per controlar l'ús i l'accés als sistemes d'informació, les aplicacions i els dipòsits de informació amb què compta la entitat? L'entitat ha definit directrius, normes i / o estàndards per controlar les terminals mòbils i accessos remots als recursos de la entitat?
Valor objectiu de l'indicador	
1	

ANNEX VI- Declaració d'Aplicabilitat del SGSI

Declaració d'Aplicabilitat del SGSI Traun

Data Publicació	Nom	Firma
23/03/2016	*Responsable de Seguretat*	TI Aprovació autor
05/04/2016	*Responsable de Riscos*	TI Aprovació revisor
08/04/2016	*Responsable de IT*	TI Aprovació

Històric de Canvis

Versió	Data Publicació	Editat per	Estat	Canvis/Comentaris
01.00	Pendent	Responsable de Seguretat	Borrador	Versió Inicial

1. Objectiu

L'objectiu d'aquest document és especificar quin dels 114 controls o mesures preventives són els que s'implementarà en Traun.

Per tant, aquest document és da servir de referència per a una auditoria de certificació on es comproven els controls implementats.

2. Abast

L' abast d'aquest procediment d'auditoria és el mateix que hi ha definit en l'abast del SGSI.

3. Declaració d'aplicabilitat

A continuació es detalla els controls de la ISO/IEC 27002:2013 que són aplicables al SGSI.

Controls	Aplicabilitat	Implementació
5. POLÍTIQUES DE LA SEGURETAT DE LA INFORMACIÓ		
5.1 Direcció de gestió de seguretat de la informació		
5.1.1 Les polítiques de seguretat de la informació	Aplica	Control necessari per la norma ISO, política seguretat de Traun
5.1.2 Revisió de les polítiques de seguretat de la informació	Aplica	Establiment periodicitat de revisió/aprovació.
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ		
6.1 Organització interna		
6.1.1 Rols i responsabilitats de seguretat de la informació	Aplica	Definit en la Politica de Seguretat
6.1.2 La segregació de funcions	Aplica	En fase de millora per part de les arees tècniques
6.1.3 Contacte amb les autoritats	Aplica	En fase de millora per part de les arees tècniques
6.1.4 Contacte amb els grups d'interès especial	Aplica	En fase de millora per part de les arees tècniques
6.1.5 Seguretat de la informació en la gestió de projectes	Aplica	Pendent de la integració de les tasques amb projectes
6.2 Els dispositius mòbils i el teletreball		
6.2.1 política de dispositiu mòbil Una política de control	Aplica	Pendent de la definició d'aquesta
6.2.2 El teletreball	Aplica	S'inicia test per part de seguretat
7. LA SEGURETAT DELS RECURSOS HUMANS		
7.1 Amb anterioritat a l'ocupació		
7.1.1 Control de Screening	Aplica	Pendent de definir
7.1.2 Termes i condicions d'ocupació	Aplica	S'utilitza l'estantard definit el l'àreea de RRHH
7.2 Durant l'ocupació		
7.2.1 Les responsabilitats de gestió	Aplica	Es troba documentat i es un document firmat per l'empleat

7.2.2 Conscienciació sobre la seguretat de la informació, l'educació i la formació	Aplica	Es comencen a definir els punts important que han de tenir en compte els usuaris
7.2.3 Procés disciplinari	Aplica	Es troba documentat i es un document firmat per l'empleat
7.3 Terminació i canvi d'ocupació		
7.3.1 La terminació o el canvi de les responsabilitats d'ocupació	Aplica	Pendent de definir
8. GESTIÓ D'ACTIUS		
8.1 La responsabilitat dels actius		
8.1.1 Inventari d'actius	Aplica	Inici d'implementació d'una CMDB
8.1.2 Propietat dels actius	Aplica	Inici d'implementació d'una CMDB
8.1.3 Ús acceptable dels actius	Aplica	Inici d'implementació d'una CMDB
8.1.4 Categories dels actius	Aplica	Inici d'implementació d'una CMDB
8.2 Classificació de la Informació		
8.2.1 Classificació de la informació	Aplica	Pendent de la implementació d'una CMDB amb la classificació
8.2.2 Etiquetatge de la informació	Aplica	Pendent de la implementació d'una CMDB amb la classificació
8.2.3 Manipulació dels procediments de control d'actius	Aplica	Pendent de la implementació d'una CMDB amb la classificació
8.3 Mitjans de manipulació		
8.3.1 Gestió de suports extraïbles	Aplica	Està definit per part de seguretat pero no es troba implementat
8.3.2 Eliminació dels mitjans	Aplica	Està definit per part de seguretat pero no es troba implementat
8.3.3 Transferència de mitjans físics	Aplica	Està definit per part de seguretat pero no es troba implementat
9. CONTROL D'ACCÉS		
9.1 Els requisits de negoci de control d'accés		
9.1.1 Política de control d'accés	Aplica	Implementat mitjançant comptes Active Directory
9.1.2 L'accés a les xarxes i serveis de xarxa	Aplica	Implementat mitjançant comptes Active Directory
9.2 Gestió d'accés dels usuaris		
9.2.1 Registre d'usuaris i baixes	Aplica	Implementat mitjançant comptes Active Directory
9.2.2 Accés aprovisionament d'usuaris	Aplica	Implementat mitjançant comptes Active Directory
9.2.3 Gestió de drets d'accés privilegiats	Aplica	Implementat mitjançant comptes Active Directory
9.2.4 Gestió de la informació de connexió de secret dels usuaris	Aplica	Implementat mitjançant comptes Active Directory
9.2.5 Revisió dels drets d'accés dels usuaris	Aplica	Es necessita un procediment per establir una revisió periòdica dels drets d'accés actuals
9.2.6 L'eliminació o ajust dels drets	Aplica	Implementat mitjançant comptes

d'accés		Active Directory
9.3 Responsabilitat dels usuaris		
9.3.1 Ús del control de la informació de connexió secreta	Aplica	Forçat per política Active Directory
9.4 Sistema de control i d'accés a les aplicacions		
9.4.1 Restricció d'accés a la informació	Aplica	Autenticació d'usuari en Active Directory directament
9.4.2 Procediments de registre en-Secure	Aplica	Pendent de desenvolupar
9.4.3 Sistema de gestió de contrasenyes	Aplica	Disposem del PMP en fase de millora
9.4.4 Ús dels programes de serveis públics privilegiats	Aplica	Pendent de desenvolupar
9.4.5 Control d'accés al codi font del programa	Aplica	Pendent de desenvolupar
10 Criptografia		
10.1 controls criptogràfics		
10.1.1 Política sobre l'ús de controls criptogràfics	Aplica	Pendent de inciar-se la utilització de tokens i definir la política
10.1.2 Gestió de claus	Aplica	S'inicia la imprementació tècnica
11 La seguretat física i ambiental		
11.1 Les àrees segures		
1.1.1 perímetre de seguretat física	Aplica	Totalment definit, implementat y en continua millora
11.1.2 controls d'entrada físiques	Aplica	Totalment definit, implementat y en continua millora
11.1.3 Protecció d'oficines, sales i instal·lacions	Aplica	Pendent de desenvolupar
11.1.4 Protecció contra amenaces externes i ambientals	Aplica	Pendent de desenvolupar
11.1.5 El treball en àrees segures	Aplica	Es troba documentat e implementat
11.1.6 Lliurament i càrrega de les zones	Aplica	Es troba documentat e implementat
11.2 Equip		
11.2.1 Emplaçament i la protecció de l'equip	Aplica	No esta establert un procediment
11.2.2 Suport als serveis públics	Aplica	Totalment definit, implementat y en continua millora
11.2.3 La seguretat de cablejat	Aplica	Implementat
11.2.4 El manteniment de l'equip	Aplica	Pendent de desenvolupar
11.2.5 Eliminació dels actius	Aplica	No esta establert un procediment on s'inclogui part de seguretat
11.2.6 Seguretat dels equips i actius fora de l'establiment	Aplica	No esta establert un procediment on s'inclogui part de seguretat
11.2.7 L'eliminació segura o la reutilització dels equips	Aplica	No esta establert un procediment
11.2.8 Equip d'usuari desatesa	Aplica	No esta establert un procediment on s'inclogui part de seguretat

11.2.9 Esborrar escriptori i la política de pantalla transparent	Aplica	S'inicia test per part de seguretat
12 Operacions de Seguretat		
12.1 Procediments i responsabilitats operacionals		
12.1.1 procediments operacionals, adequadament documentats	Aplica	Totalment definit, implementat y en continua millora
12.1.2 Gestió de canvis	Aplica	Totalment definit, implementat y en continua millora
12.1.3 Capacitat de gestió	Aplica	Totalment definit, implementat y en continua millora
12.1.4 Separació de desenvolupament, prova i entorns operatius	Aplica	Totalment definit, implementat y en continua millora
12.2 Protecció contra el malware		
12.2.1 Controls contra el malware	Aplica	Es disposa d'antivirus, proxy, firewall e IPS
12.3 Còpia de seguretat		
12.3.1 Informació de còpia de seguretat	Aplica	S'utilitza l'eina Data protector, però no es troba definida una política de backups
12.4 Registre i supervisió		
12.4.1 registre d'esdeveniments	Aplica	Totalment definit, implementat y en continua millora
12.4.2 Protecció de la informació de registre	Aplica	Totalment definit, implementat y en continua millora
12.4.3 Administrador i operador registres	Aplica	Totalment definit, implementat y en continua millora
12.4.4 Sincronització del rellotge	Aplica	Totalment definit, implementat y en continua millora
12.5 de control de programari operacional		
12.5.1 Instal·lació de programari en sistemes operatius	Aplica	Totalment definit, implementat y en continua millora
12.6 La gestió tècnica de la vulnerabilitat		
12.6.1 Gestió de vulnerabilitats tècniques	Aplica	Totalment definit, implementat y en continua millora
12.6.2 Restriccions en la instal·lació del programari	Aplica	Totalment definit, implementat y en continua millora
12.7 Sistemes d'informació consideracions d'auditoria		
12.7.1 Sistemes d'informació controls d'auditoria	Aplica	Pendent de desenvolupar
13 Seguretat de les comunicacions		
13.1 de gestió de seguretat de xarxa		
13.1.1 controls de xarxa	Aplica	Es disposa d'antivirus, proxy, firewall e IPS
13.1.2 Seguretat dels serveis de xarxa	Aplica	Es disposa d'antivirus, proxy, firewall e IPS
13.1.3 La segregació a les xarxes	Aplica	Separació de xarxes i creació de subxarxes

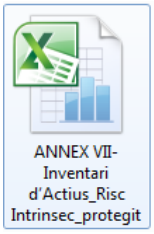
13.2 La transferència d'informació		
13.2.1 polítiques i procediments de transferència d'informació	Aplica	Es troba documentat e implementat
13.2.2 Els acords sobre la transferència d'informació	Aplica	Es troba documentat e implementat
13.2.3 La missatgeria electrònica	Aplica	Totalment definit, implementat y en continua millora
13.2.4 Confidencialitat o de no divulgació acords	Aplica	Es troba documentat e implementat
14 Sistema d'adquisició, desenvolupament i manteniment		
14.1 Els requisits de seguretat dels sistemes d'informació		
14.1.1 Informació d'anàlisi de requisits de seguretat i les especificacions	Aplica	Pendent de desenvolupar
14.1.2 serveis d'aplicacions de fixació de les xarxes públiques	Aplica	Pendent de desenvolupar
14.1.3 Protecció de les transaccions de serveis d'aplicacions	Aplica	Pendent de desenvolupar
14.2 Seguretat en els processos de desenvolupament i suport		
14.2.1 política de desenvolupament segur	Aplica	Pendent de desenvolupar
14.2.2 els procediments de control de canvis del Sistema	Aplica	Pendent de desenvolupar
14.2.3 Revisió tècnica d'aplicacions després de canvis en la plataforma d'operació	Aplica	Es realitzar, no es troba procedimentat
14.2.4 Les restriccions als canvis en els paquets de programari	Aplica	Pendent de desenvolupar
14.2.5 principis d'enginyeria de sistemes segurs	Aplica	Pendent de desenvolupar
14.2.6 entorn de desenvolupament segur	Aplica	Pendent de desenvolupar
14.2.7 Desenvolupament externalitzat	Aplica	Pendent de desenvolupar
14.2.8 Les proves de seguretat del sistema	Aplica	Es realitzar per la part de vulnerabilitats
14.2.9 Sistema de proves d'acceptació	Aplica	Pendent de desenvolupar
14.3 Les dades de prova		
14.3.1 Protecció de dades de prova	Aplica	No esta establert un procediment
15 Les relacions amb proveïdors		
15.1 Seguretat de la informació en relació amb els proveïdors		
15.1.1 La política de seguretat de la informació de relacions amb els proveïdors	Aplica	Es troba documentat e implementat
15.1.2 Abordar la seguretat dins dels acords amb proveïdors	Aplica	Es troba documentat e implementat
15.1.3 Cadena de la tecnologia d'informació i comunicació de subministrament	Aplica	Es troba documentat e implementat

15.2 La gestió de la prestació de serveis de proveïdors		
15.2.1 Seguiment i revisió dels serveis de proveïdors	Aplica	Pendent de desenvolupar
15.2.2 Gestió de canvis en els serveis de proveïdors	Aplica	Pendent de desenvolupar
16 Gestió d'incidents de seguretat d'informació		
16.1 Gestió dels incidents de seguretat de la informació i millores		
16.1.1 Responsabilitats i procediments	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.2 Informes esdeveniments de seguretat de la informació	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.3 Informes debilitats de seguretat d'informació	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.4 L'avaluació i la decisió sobre els esdeveniments de seguretat d'informació	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.5 Resposta a incidents de seguretat d'informació de control	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.6 Aprenent dels incidents de seguretat de la informació	Aplica	Pendent de la subcontractació d'una empresa externa
16.1.7 Reunió de proves	Aplica	Pendent de la subcontractació d'una empresa externa
17 Aspectes de seguretat d'informació de gestió de la continuïtat del negoci		
17.1 La continuïtat seguretat de la informació		
17.1.1 Planificació de la continuïtat seguretat de la informació	Aplica	Totalment definit, implementat y en continua millora
17.1.2 Implementació de la informació de seguretat de continuïtat	Aplica	Totalment definit, implementat y en continua millora
17.1.3 Verificar, revisar i avaluar la informació de seguretat de continuïtat	Aplica	Totalment definit, implementat y en continua millora
17.2 Les redundàncies		
17.2.1 Disponibilitat d'instal·lacions de processament d'informació	Aplica	Totalment definit, implementat y en continua millora
18 Compliment		
18.1 El compliment dels requisits legals i contractuals		
18.1.1 Identificació de la legislació aplicable i els requisits contractuals	Aplica	Totalment definit, implementat y en continua millora
18.1.2 Drets de propietat intel·lectual	Aplica	Totalment definit, implementat y en continua millora
18.1.3 Registres de control de registres	Aplica	Totalment definit, implementat y en continua millora
18.1.4 Privacitat i protecció de dades personals	Aplica	Totalment definit, implementat y en continua millora
18.1.5 Regulació de controls criptogràfics	Aplica	Totalment definit, implementat y en continua millora
18.2 opinions seguretat de la informació		
18.2.1 Revisió independent de la	Aplica	Totalment definit, implementat y en

seguretat de la informació		continua millora
18.2.2 El compliment de les polítiques i normes de seguretat	Aplica	Totalment definit, implementat y en continua millora
18.2.3 Revisió de compliment tècnic	Aplica	Totalment definit, implementat y en continua millora

ANNEX VII- Inventari d'Actius i Risc Intrínsec

S'adjunta amb el TFM un Excel (*ANNEX VII- Inventari d'Actius_Risc Intrinsec_protegit.xlsx*) on podreu trobar l'inventari d'actius, la valoració d'actius i els risc intrínsec. També trobareu altres fulles d'Excel que han sigut incorporades el TFM en el ANNEXES VII, IX i X.



ANNEX VIII- Anàlisis d'amenaces

Tipus	Codi	Amenaça	Actiu Afectat							
			I	HW	SW	D	X	S	EA	P
Amenaces d'origen natural	AM-01	Incendi	X	X					X	
	AM-02	Inundació	X	X					X	
	AM-03	Desastre natural	X	X					X	
	AM-04	Atac físic	X	X					X	
	AM-05	Fallada / avaria d'equip	X	X					X	
	AM-06	Avaria climatització	X	X					X	
	AM-07	Errades subministrament elèctric	X	X					X	
Amenaces d'entorn o d'origen industrial	AM-08	Robatori personal intern		X	X					
	AM-09	Manipulació d'equipament		X	X					
	AM-10	indisponiblitat física	X	X			X		X	X
	AM-11	indisponiblitat lògica			X	X				
	AM-12	indisponiblitat personal								X
	AM-13	Indisponiblitat de comunicacions					X			
Errors i errors no intencionats	AM-14	Error de disseny			X	X				
	AM-15	Manca de manteniment programari			X	X	X			
	AM-16	Errors humans	X	X	X	X	X	X	X	X
	AM-17	Pèrdua d'informació				X				
	AM-18	Pèrdua de documents				X				X
	AM-19	Fallades de programari			X	X				
	AM-20	Fallada en còpies		X	X	X				
	AM-21	Fallada en les comunicacions					X			
Atacs intencionats	AM-22	Eliminació no autoritzada				X				X

	AM-23	Robatori persones externes			X	X				X
	AM-24	Atac informàtic		X	X	X	X	X		
	AM-25	Coacció				X				X
	AM-26	Negligència	X	X	X	X	X			X
	AM-27	Difusió a persones no autoritzades				X				X
	AM-28	Accés no autoritzat a sistemes			X	X				X
	AM-29	Enginyeria inversa		X	X	X				
	AM-30	Divulgació no autoritzada	X	X	X	X	X	X	X	X

ANNEX IX- Anàlisis d'actius vs amenaces.

A continuació detalles els actius vs les amenaces d'origen natural segons la freqüència.

		Incendi		Inundació		Desastre natural		Atac físic		Fallada / avaria d'equip		Avaria climatització		Errades subministrament elèctric	
Codi	**Actiu**	**AM-01**		**AM-02**		**AM-03**		**AM-04**		**AM-05**		**AM-06**		**AM-07**	
I.1	CPD	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	PF	0,010959
I.2	Llocs de treball corporatius	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	F	0,016438
I.3	Llocs de direcció	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	PF	0,010959
I.4	Llocs de treball divisió d'operació	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	F	0,016438
I.5	Llocs de treball divisió industrial	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	PF	0,010959
I.6	Llocs de treball comercial	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	F	0,016438
I.7	Sales d'impressió	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	F	0,016438
HW.1	Firewalls	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.2	Proxys	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.3	Siem	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740

HW.4	IPS	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.5	Qualys	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.6	Load Balancer	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.7	Routers	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.8	Impresores	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.9	Workstations	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.10	Laptops	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.11	Mòbils	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.12	AIX 6	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.13	Cabina de discos SATA – Dades	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.14	VMWARE ESXi	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.15	Backups	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
HW.16	Commutadors xarxa	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
SW.1	SCADA	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.2	Windows 7	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.3	Windows Server 2003	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.4	Windows server 2008 R2	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.5	Windows server 2012 R2	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.6	Red Hat Enterprise Linux 5.9	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.7	Red Hat Enterprise Linux 6.5	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.8	Red Hat Enterprise Linux 6.7	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.9	Apache Tomcat	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.10	IIS	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.11	SQL	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.12	Oracle 10g	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.13	Oracle 11g	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.14	Oracle 12c	-	0	-	0	-	0	-	0	-	0	-	0	-	0

SW.15	Solaris 11	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.16	AD RHH	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.17	SAP	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.18	Antivirus	-	0	-	0	-	0	-	0	-	0	-	0	-	0
SW.19	HP Data Protector	-	0	-	0	-	0	-	0	-	0	-	0	-	0
D.1	Backups	-	0	-	0	-	0	-	0	-	0	-	0	-	0
D.2	Documentum	-	0	-	0	-	0	-	0	-	0	-	0	-	0
D.3	DMS	-	0	-	0	-	0	-	0	-	0	-	0	-	0
D.4	GDS	-	0	-	0	-	0	-	0	-	0	-	0	-	0
X.1	ADSL	-	0	-	0	-	0	-	0	-	0	-	0	-	0
X.2	Routers Wifi	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.1	GDS	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.2	AD RRHH	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.3	Impresores	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.4	Exchange	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.5	Webs	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.6	Viatjes	-	0	-	0	-	0	-	0	-	0	-	0	-	0
S.7	Formació	-	0	-	0	-	0	-	0	-	0	-	0	-	0
EA.1	Armaris rack CPD	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
EA.2	Refrigeració CPD	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
EA.3	Side	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740
P.1	Director TI	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.2	Responsable de Riscos	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.3	Tècnics INTEL	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.4	Tècnics UNIX	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.5	Tècnics web	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.6	Tècnics BBDD	-	0	-	0	-	0	-	0	-	0	-	0	-	0

P.7	Tècnics SAP	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.8	Tècnics de Xarxes	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.9	Tècnics d'operacions	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.10	Tècnics de monitoring	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.11	Tècnics de backup	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.12	Tècnics Seguretat i antivirus	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.13	Tècnics de desenvolupament	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.14	Tècnics Acive Directory	-	0	-	0	-	0	-	0	-	0	-	0	-	0
P.15	Tècnics SCCM	-	0	-	0	-	0	-	0	-	0	-	0	-	0

A continuació detalles els actius vs les amenaces d'entorn o d'origen industrial segons la freqüència.

		Robatori personal intern		Manipulació d'equipament		indisponibilitat física		indisponibilitat lògica		indisponibilitat personal		Indisponibilitat de comunicacions	
Codi	**Actiu**	**AM-08**		**AM-09**		**AM-10**		**AM-11**		**AM-12**		**AM-13**	
I.1	CPD	-	0	-	0	D	0,002740	-	0	-	0	-	0
I.2	Llocs de treball corporatius	-	0	-	0	D	0,002740	-	0	-	0	-	0
I.3	Llocs de direcció	-	0	-	0	D	0,002740	-	0	-	0	-	0

I.4	Llocs de treball divisió d'operació	-	0	-	0	D	0,002740	-	0	-	0	-	0
I.5	Llocs de treball divisió industrial	-	0	-	0	D	0,002740	-	0	-	0	-	0
I.6	Llocs de treball comercial	-	0	-	0	D	0,002740	-	0	-	0	-	0
I.7	Sales d'impressió	-	0	-	0	D	0,002740	-	0	-	0	-	0
HW.1	Firewalls	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.2	Proxys	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.3	Siem	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.4	IPS	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.5	Qualys	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.6	Load Balancer	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.7	Routers	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.8	Impresores	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.9	Workstations	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.10	Laptops	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.11	Mòbils	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.12	AIX 6	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.13	Cabina de discos SATA – Dades	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.14	VMWARE ESXi	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.15	Backups	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
HW.16	Commutadors xarxa	D	0,002740	F	0,016438	MPF	0,005479	-	0	-	0	-	0
SW.1	SCADA	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.2	Windows 7	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.3	Windows Server 2003	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.4	Windows server 2008 R2	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.5	Windows server 2012 R2	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.6	Red Hat Enterprise Linux 5.9	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.7	Red Hat Enterprise Linux 6.5	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0

SW.8	Red Hat Enterprise Linux 6.7	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.9	Apache Tomcat	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.10	IIS	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.11	SQL	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.12	Oracle 10g	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.13	Oracle 11g	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.14	Oracle 12c	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.15	Solaris 11	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.16	AD RHH	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.17	SAP	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.18	Antivirus	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
SW.19	HP Data Protector	MPF	0,005479	MF	0,071233	-	0	F	0,016438	-	0	-	0
D.1	Backups	-	0	-	0	-	0	D	0,002740	-	0	-	0
D.2	Documentum	-	0	-	0	-	0	D	0,002740	-	0	-	0
D.3	DMS	-	0	-	0	-	0	D	0,002740	-	0	-	0
D.4	GDS	-	0	-	0	-	0	D	0,002740	-	0	-	0
X.1	ADSL	-	0	-	0		0,000000	-	0	-	0	MF	0,071233
X.2	Routers Wifi	-	0	-	0		0,000000	-	0	-	0	MF	0,071233
S.1	GDS	-	0	-	0	-	0	-	0	-	0	-	0
S.2	AD RRHH	-	0	-	0	-	0	-	0	-	0	-	0
S.3	Impresores	-	0	-	0	-	0	-	0	-	0	-	0
S.4	Exchange	-	0	-	0	-	0	-	0	-	0	-	0
S.5	Webs	-	0	-	0	-	0	-	0	-	0	-	0
S.6	Viatjes	-	0	-	0	-	0	-	0	-	0	-	0
S.7	Formació	-	0	-	0	-	0	-	0	-	0	-	0
EA.1	Armaris rack CPD	-	0	-	0	MPF	0,005479	-	0	-	0	-	0
EA.2	Refrigeració CPD	-	0	-	0	MPF	0,005479	-	0	-	0	-	0

EA.3	Side	-	0	-	0	MPF	0,005479	-	0	-	0	-	0
P.1	Director TI	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.2	Responsable de Riscos	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.3	Tècnics INTEL	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.4	Tècnics UNIX	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.5	Tècnics web	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.6	Tècnics BBDD	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.7	Tècnics SAP	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.8	Tècnics de Xarxes	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.9	Tècnics d'operacions	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.10	Tècnics de monitoring	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.11	Tècnics de backup	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.12	Tècnics Seguretat i antivirus	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.13	Tècnics de desenvolupament	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.14	Tècnics Acive Directory	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0
P.15	Tècnics SCCM	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0

A continuació detalles els actius vs les amenaces d'errors i errors no intencionats segons la freqüència.

		Error de disseny		Manca de manteniment programari		Errors humans		Pèrdua d'informació		Pèrdua de documents		Fallades de programari		Fallada en còpies		Fallada en les comunicacions	
Codi	**Actiu**	**AM-14**		**AM-15**		**AM-16**		**AM-17**		**AM-18**		**AM-19**		**AM-20**		**AM-21**	
I.1	CPD	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.2	Llocs de treball corporatius	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.3	Llocs de direcció	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.4	Llocs de treball divisió d'operació	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.5	Llocs de treball divisió industrial	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.6	Llocs de treball comercial	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
I.7	Sales d'impressió	-	0	-	0	D	0,002740	-	0	-	0	-	0	-	0	-	0
HW.1	Firewalls	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.2	Proxys	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.3	Siem	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.4	IPS	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.5	Qualys	-	0	-	0	D	0,002740	-	0	-	0	-	0	EF	1,000000	-	0
HW.6	Load Balancer	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.7	Routers	-	0	-	0	D	0,002740	-	0	-	0	-	0	MPF	0,005479	-	0
HW.8	Impresores	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0

HW.9	Workstations	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.10	Laptops	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.11	Mòbils	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.12	AIX 6	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.13	Cabina de discos SATA – Dades	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.14	VMWARE ESXi	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.15	Backups	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
HW.16	Commutadors xarxa	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740	-	0
SW.1	SCADA	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.2	Windows 7	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.3	Windows Server 2003	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.4	Windows server 2008 R2	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.5	Windows server 2012 R2	F	0,016438	F	0,016438	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.6	Red Hat Enterprise Linux 5.9	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.7	Red Hat Enterprise Linux 6.5	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.8	Red Hat Enterprise Linux 6.7	F	0,016438	F	0,016438	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.9	Apache Tomcat	F	0,016438	F	0,016438	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.10	IIS	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.11	SQL	F	0,016438	F	0,016438	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.12	Oracle 10g	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.13	Oracle 11g	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.14	Oracle 12c	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0

SW.15	Solaris 11	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.16	AD RHH	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.17	SAP	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.18	Antivirus	F	0,016438	MF	0,071233	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
SW.19	HP Data Protector	F	0,016438	EF	1,000000	MPF	0,005479	-	0	-	0	D	0,002740	D	0,002740	-	0
D.1	Backups	F	0,016438	MPF	0,005479	MPF	0,005479	D	0,002740	D	0,002740	D	0,002740	D	0,002740	-	0
D.2	Documentum	F	0,016438	MF	0,071233	MPF	0,005479	D	0,002740	D	0,002740	D	0,002740	D	0,002740	-	0
D.3	DMS	F	0,016438	MPF	0,005479	MPF	0,005479	D	0,002740	D	0,002740	D	0,002740	D	0,002740	-	0
D.4	GDS	F	0,016438	D	0,002740	MPF	0,005479	D	0,002740	D	0,002740	D	0,002740	D	0,002740	-	0
X.1	ADSL	-	0	F	0,016438	MPF	0,005479	-	0	-	0	-	0	-	0	MPF	0,005479
X.2	Routers Wifi	-	0	MPF	0,005479	MPF	0,005479	-	0	-	0	-	0	-	0	MPF	0,005479
S.1	GDS	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.2	AD RRHH	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.3	Impresores	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.4	Exchange	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.5	Webs	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.6	Viatjes	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
S.7	Formació	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
EA.1	Armaris rack CPD	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
EA.2	Refrigeració CPD	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
EA.3	Side	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	-	0	-	0
P.1	Director TI	-	0	-	0	MPF	0,005479	-	0	D	0,002740	-	0	-	0	-	0
P.2	Responsable de Riscos	-	0	-	0	MPF	0,005479	-	0	D	0,002740	-	0	-	0	-	0

P.3	Tècnics INTEL	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.4	Tècnics UNIX	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.5	Tècnics web	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.6	Tècnics BBDD	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.7	Tècnics SAP	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.8	Tècnics de Xarxes	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.9	Tècnics d'operacions	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.10	Tècnics de monitoring	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.11	Tècnics de backup	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.12	Tècnics Seguretat i antivirus	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.13	Tècnics de desenvolupament	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.14	Tècnics Acive Directory	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0
P.15	Tècnics SCCM	-	0	-	0	MPF	0,005479	-	0	MPF	0,005479	-	0	-	0	-	0

A continuació detalles els actius vs les amenaces d'atacs intencionats segons la freqüència:

		Eliminacion no autoritzada		Robatori persones externes		Atac informàtic		Coacció		Negligència		Difusion a persones no autoritzades		Accés no autoritzat a sistemes		Enginyeria inversa		Divulgació no autoritzada	
Codi	**Actiu**	**AM-22**		**AM-23**		**AM-24**		**AM-25**		**AM-26**		**AM-27**		**AM-28**		**AM-29**		**AM-30**	
I.1	CPD	-	0	-	0	-	0	-	0	D	0,002740	-	0	-	0	-	0	D	0,002740
I.2	Llocs de treball corporatius	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0	-	0	D	0,002740
I.3	Llocs de direcció	-	0	-	0	-	0	-	0	MPF	0,005479	-	0	-	0	-	0	D	0,002740
I.4	Llocs de treball divisió d'operació	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0	-	0	D	0,002740
I.5	Llocs de treball divisió industrial	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0	-	0	D	0,002740
I.6	Llocs de treball comercial	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0	-	0	D	0,002740
I.7	Sales d'impressió	-	0	-	0	-	0	-	0	F	0,016438	-	0	-	0	-	0	D	0,002740
HW.1	Firewalls	-	0	-	0	F	0,016438	-	0	MPF	0,005479	-	0	-	0	MPF	0,005479	MPF	0,005479
HW.2	Proxys	-	0	-	0	F	0,016438	-	0	F	0,016438	-	0	-	0	MPF	0,005479	MPF	0,005479

HW.3	Siem	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.4	IPS	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.5	Qualys	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.6	Load Balancer	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.7	Routers	-	0	-	0	F	0,016438	-	0	F	0,016438	-	0	-	0	MPF	0,005479	MPF	0,005479
HW.8	Impresores	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0	MPF	0,005479	MPF	0,005479
HW.9	Workstations	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0	MPF	0,005479	MPF	0,005479
HW.10	Laptops	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0	D	0,002740	MPF	0,005479
HW.11	Mòbils	-	0	-	0	D	0,002740	-	0	F	0,016438	-	0	-	0	MPF	0,005479	MPF	0,005479
HW.12	AIX 6	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.13	Cabina de discos SATA – Dades	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.14	VMWARE ESXi	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.15	Backups	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
HW.16	Commutadors xarxa	-	0	-	0	D	0,002740	-	0	D	0,002740	-	0	-	0	D	0,002740	MPF	0,005479
SW.1	SCADA	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	F	0,016438	MPF	0,005479	MPF	0,005479

SW.2	Windows 7	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	F	0,016438	D	0,002740	MPF	0,005479
SW.3	Windows Server 2003	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.4	Windows server 2008 R2	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.5	Windows server 2012 R2	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.6	Red Hat Enterprise Linux 5.9	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.7	Red Hat Enterprise Linux 6.5	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.8	Red Hat Enterprise Linux 6.7	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.9	Apache Tomcat	-	0	D	0,002740	MPF	0,005479	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.10	IIS	-	0	D	0,002740	MPF	0,005479	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.11	SQL	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.12	Oracle 10g	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	F	0,016438	D	0,002740	MPF	0,005479
SW.13	Oracle 11g	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	F	0,016438	D	0,002740	MPF	0,005479
SW.14	Oracle 12c	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	F	0,016438	D	0,002740	MPF	0,005479
SW.15	Solaris 11	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.16	AD RHH	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479

SW.17	SAP	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.18	Antivirus	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
SW.19	HP Data Protector	-	0	D	0,002740	D	0,002740	-	0	D	0,002740	-	0	MPF	0,005479	D	0,002740	MPF	0,005479
D.1	Backups	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	MPF	0,005479
D.2	Documentum	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	MPF	0,005479
D.3	DMS	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	MPF	0,005479
D.4	GDS	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	D	0,002740	MPF	0,005479
X.1	ADSL	-	0	-	0	MPF	0,005479	-	0	D	0,002740	-	0	-	0	-	0	F	0,016438
X.2	Routers Wifi	-	0	-	0	MPF	0,005479	-	0	D	0,002740	-	0	-	0	-	0	F	0,016438
S.1	GDS	-	0	-	0	D	0,002740	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
S.2	AD RRHH	-	0	-	0	D	0,002740	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
S.3	Impresores	-	0	-	0	D	0,002740	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
S.4	Exchange	-	0	-	0	F	0,016438	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
S.5	Webs	-	0	-	0	MPF	0,005479	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
S.6	Viatjes	-	0	-	0	D	0,002740	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479

S.7	Formació	-	0	-	0	D	0,002740	-	0	-	0,000000	-	0	-	0	-	0	MPF	0,005479
EA.1	Armaris rack CPD	-	0	-	0	-	0	-	0	-	0,000000	-	0	-	0	-	0	D	0,002740
EA.2	Refrigeració CPD	-	0	-	0	-	0	-	0	-	0,000000	-	0	-	0	-	0	D	0,002740
EA.3	Side	-	0	-	0	-	0	-	0	-	0,000000	-	0	-	0	-	0	D	0,002740
P.1	Director TI	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	MPF	0,005479	D	0,002740	-	0	D	0,002740
P.2	Responsable de Riscos	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	D	0,002740	D	0,002740	-	0	D	0,002740
P.3	Tècnics INTEL	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.4	Tècnics UNIX	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.5	Tècnics web	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.6	Tècnics BBDD	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.7	Tècnics SAP	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.8	Tècnics de Xarxes	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.9	Tècnics d'operacions	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.10	Tècnics de monitoring	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.11	Tècnics de backup	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740

P.12	Tècnics Seguretat i antivirus	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.13	Tècnics de desenvolupament	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.14	Tècnics Acive Directory	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740
P.15	Tècnics SCCM	D	0,002740	MPF	0,005479	-	0	D	0,002740	MPF	0,005479	F	0,016438	D	0,002740	-	0	D	0,002740

ANNEX X- Anàlisis d'actius vs Impacte Potencial

Àmbit	Codi	Quantitat	Actiu	Valor Qualitatiu	Valor Quantitatiu	Impacte Qualitatiu	Impacte	Impacte Potencial
Instal·lacions	I.1	4	CPD	MA	300000	C	0,900	270000
	I.2	38	Llocs de treball corporatius	A	150000	M	0,500	75000
	I.3	3	Llocs de direcció	A	150000	A	0,750	112500
	I.4	50	Llocs de treball divisó d'operació	M	75000	B	0,200	15000
	I.5	15	Llocs de treball divisó industrial	A	150000	A	0,750	112500
	I.6	10	Llocs de treball comercial	B	30000	B	0,200	6000
	I.7	38	Sales d'impressió	MB	10000	B	0,200	2000
Hardware	HW.1	12	Firewalls	A	150000	A	0,750	112500
	HW.2	5	Proxys	M	75000	B	0,200	15000
	HW.3	6	Siem	M	75000	M	0,500	37500
	HW.4	3	IPS	M	75000	M	0,500	37500
	HW.5	4	Qualys	M	75000	B	0,200	15000
	HW.6	15	Load Balancer	M	75000	B	0,200	15000
	HW.7	150	Routers	M	75000	M	0,500	37500
	HW.8	115	Impresores	MB	10000	B	0,200	2000
	HW.9	600	Workstations	M	75000	B	0,200	15000
	HW.10	2500	Laptops	M	75000	B	0,200	15000
	HW.11	1000	Mòbils	MB	10000	B	0,200	2000
	HW.12	50	AIX 6	MA	300000	M	0,500	150000
	HW.13	8	Cabina de discos SATA – Dades	MA	300000	M	0,500	150000
	HW.14	102	VMWARE ESXi	MA	300000	A	0,750	225000
	HW.15	2	Backups	A	150000	A	0,750	112500
	HW.16	6	Commutadors xarxa	A	150000	B	0,200	30000
Aplicació i software	SW.1	200	SCADA	MA	300000	C	0,900	270000
	SW.2	3900	Windows 7	M	75000	M	0,500	37500
	SW.3	136	Windows Server 2003	MB	10000	M	0,500	5000
	SW.4	530	Windows server 2008 R2	MA	300000	M	0,500	150000
	SW.5	95	Windows server 2012 R2	MA	300000	M	0,500	150000

	SW.6	18	Red Hat Enterprise Linux 5.9	M	75000	M	0,500	37500
	SW.7	116	Red Hat Enterprise Linux 6.5	A	150000	M	0,500	75000
	SW.8	36	Red Hat Enterprise Linux 6.7	MA	300000	M	0,500	150000
	SW.9	148	Apache Tomcat	A	150000	M	0,500	75000
	SW.10	29	IIS	A	150000	M	0,500	75000
	SW.11	78	SQL	A	150000	M	0,500	75000
	SW.12	45	Oracle 10g	M	75000	M	0,500	37500
	SW.13	92	Oracle 11g	A	150000	M	0,500	75000
	SW.14	37	Oracle 12c	MA	300000	M	0,500	150000
	SW.15	63	Solaris 11	M	75000	M	0,500	37500
	SW.16	2	AD RHH	M	75000	M	0,500	37500
	SW.17	26	SAP	A	150000	M	0,500	75000
	SW.18	1	Antivirus	M	75000	M	0,500	37500
	SW.19	4000	HP Data Protector	MA	300000	M	0,500	150000
Dades	D.1	8	Backups	MA	300000	C	0,900	270000
	D.2	6	Documentum	M	75000	B	0,200	15000
	D.3	3	DMS	MA	300000	C	0,900	270000
	D.4	2	GDS	MA	300000	C	0,900	270000
Xarxa	X.1	153	ADSL	M	75000	A	0,750	56250
	X.2	120	Routers Wifi	M	75000	A	0,750	56250
Serveis	S.1	2	GDS	A	150000	C	0,900	135000
	S.2	2	AD RRHH	M	75000	M	0,500	37500
	S.3	160	Impresores	MB	10000	B	0,200	2000
	S.4	4	Exchange	M	75000	C	0,900	67500
	S.5	2	Webs	B	30000	C	0,900	27000
	S.6	2	Viatjes	MB	10000	B	0,200	2000
	S.7	2	Formació	MB	10000	B	0,200	2000
Equipament auxiliar	EA.1	12	Armaris rack CPD	M	75000	C	0,900	67500
	EA.2	8	Refrigeració CPD	B	30000	C	0,900	27000
	EA.3	8	Side	B	30000	C	0,900	27000
Personal	P.1	1	Director TI	MA	300000	A	0,750	225000
	P.2	2	Responsable de Riscos	MA	300000	M	0,500	150000
	P.3	18	Tècnics INTEL	A	150000	A	0,750	112500
	P.4	12	Tècnics UNIX	A	150000	A	0,750	112500
	P.5	5	Tècnics web	M	75000	M	0,500	37500
	P.6	4	Tècnics BBDD	MA	300000	A	0,750	225000
	P.7	2	Tècnics SAP	A	150000	M	0,500	75000
	P.8	8	Tècnics de Xarxes	A	150000	A	0,750	112500

	P.9	10	Tècnics d'operacions	M	75000	M	0,500	37500
	P.10	7	Tècnics de monitoring	M	75000	M	0,500	37500
	P.11	3	Tècnics de backup	MA	300000	M	0,500	150000
	P.12	7	Tècnics Seguretat i antivirus	M	75000	M	0,500	37500
	P.13	11	Tècnics de desenvolupament	B	30000	B	0,200	6000
	P.14	3	Tècnics Acive Directory	M	75000	B	0,200	15000
	P.15	6	Tècnics SCCM	M	75000	B	0,200	15000

ANNEX XI- Projectes a curt termini

S'adjunta amb el TFM un PDF (*ANNEX XI- Projectes a curt termini.pdf*) on podreu trobar els projectes a curt termini, el seu cost total, els resultats, la planificació i la implementació.

ANNEX XII- Projectes a mig termini

S'adjunta amb el TFM un PDF (*ANNEX XII- Projectes a mig termini.pdf*) on podreu trobar els projectes a mig termini, el seu cost total, els resultats, la planificació i la implementació.

ANNEX XIII- Projectes a llarg termini

S'adjunta amb el TFM un PDF (*ANNEX XIII- Projectes a llarg termini.pdf*) on podreu trobar els projectes a llarg termini, el seu cost total, els resultats, la planificació i la implementació.

ANNEX XIV- Informe d'Auditoria

INFORME D'AUDITORIA TRAUN

1. Informe executiu

El servei d'auditoria de seguretat contra el referencial ISO 27002 analitza la seguretat de la informació d'una organització, sigui del tipus que sigui i sigui de la mida que sigui, 114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius.

El resultat de l'auditoria estableix, en tots els àmbits de protecció: físic, lògic, organitzatiu i legal, l'estat de seguretat d'una organització en un moment donat del temps.

Aquest nivell de seguretat quantitatiu en base a una avaluació objectiva de l'estat de la seguretat permet a l'organització establir un full de ruta per assolir el seu objectiu de seguretat alineat amb el seu enfocament estratègic, li permet comparar-ne amb altres organitzacions del mateix sector o d'una regió geogràfica o establir el grau de millora contínua en la base de la implantació de salvaguardes o controls que de forma gradual es van definint.

2. Identificació del beneficiari

A continuació es presenten les dades bàsiques de la Organització:

NOM	TRAUN.SL
DATA	2019
CONTRACTE	2018-1-ES1-ERA12-487A
EMPLAÇAMENT DE L'AUDITORIA	C./ TAJO 45
	08191 - RUBÍ
PERSONES ENTREVISTADES	10

3. Abast

L'abast serà tots els controls aplicables en l'ANNEX VI, Declaració d'Aplicabilitat del SGSI.

4. Equip Auditor

El requisit fonamental per a la selecció de l'equip auditor era que tingués la màxima imparcialitat i objectivitat.

Auditora: Maria Ponce León

5. Dates d'execució de l'Auditoria

Aquesta auditoria s'ha realitzat entre el 14 gener 2019 i el 18 febrer 2019
Els diferents períodes i tasques realitzats són:

Inici	Final	Tasques
14-ene.	18-ene.	Recull d'informació, així com l'estudi de la mateixa.
21-ene.	8-feb.	Realització d'entrevistes, visites i proves tècniques.
11-feb.	18-feb.	Anàlisi de la Informació i Elaboració d'Informes.

6. Normativa emprada

Aquesta Auditoria es realitza respecte a als 114 controls o mesures preventives , organitzats en 14 àrees i 35 objectius de control de la i ISO/IEC 27002, i ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

Aquesta valoració la realitzarem segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem.
10%	L1	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal.
50%	L2	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca.
90%	L3	Procés definit	La organització sencera participa al procés.
95%	L4	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
100%	L5	Optimitzat	Els processos estan sota constant millora.

7. Informe detallat

A continuació analitzarem cada control, la feina realitzada, les observacions i les conclusions:

Àrea	5. Polítiques de la Seguretat de la Informació	Conclusió	Conforme

Control ISO/IEC 27002:2013: 5.1 Direcció de gestió de seguretat de la informació
Proporcionar orientació i suport per a seguretat de la informació, d'acord amb els requeriments del negoci i les lleis i reglaments pertinents de gestió.

Treball realitzat
És revisa l'existència d'una política de Seguretat.

Observació
Es verifica l'existència d'una política de Seguretat aprovada per l'administració, i publicat i comunicat a tots els empleats i col·laboradors externs.

Evidencies
És detallen les evidencies recollides: ▪ **EV_001:** Document Política de Seguretat publicat al 17/03/2016

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	6.Organització de la seguretat de la informació	Conclusió	Conforme

Control ISO/IEC 27002:2013: 6.1 Organització interna
Un marc de gestió ha de ser establerta per iniciar i controlar l'aplicació de seguretat de la informació dins de l'organització

Treball realitzat
És revisa els frameworks de seguretat establerts per iniciar i controlar l'aplicació de seguretat de la informació dins de l'organització.

Observació
Es verifica que Traun disposa de diferents frameworks, s'analitza algunes mostres per validar el seu funcionament i la seva aplicabilitat.

Evidencies
És detallen les evidencies recollides: ▪ **EV002**: Frameworks de seguretat corporativa.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	6.Organització de la seguretat de la informació	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 6.2 Els dispositius mòbils i el teletreball
Per garantir la seguretat del teletreball i l'ús de dispositius mòbils.

Treball realitzat
És revisa la plantilla corporativa de la telefonia, en aquest cas ios. És revisa les VPN i el mètode d'autenticació mitjançant RSA per a la realització de teletraball.

Observació
La plantilla corporativa de ios no es troba securitzada, així mateix, tampoc hi ha una guia de seguretat i bon ús dels dispositius mòbils.

Evidencies
És detallen les evidencies recollides: ▪ **EV003:** Procediment de Desplegament de RSA. ▪ **EV004:**Documents d'instruccions operacionals de com connectar-se per a la realització de teletraball.

Recomanació
És recomana generar instruccions pel que fa a l'antivirus en el cas de que el actiu s'hagi connectat a traves d'una red publica.

Estat	En curs	Responsable	Ivan R.	Termini	3 mesos

Àrea	7. La seguretat dels recursos humans	Conclusió	Conforme

Control ISO/IEC 27002:2013: 7.1 Amb anterioritat a l'ocupació
Garantir que els empleats i contractistes a entendre les seves responsabilitats i són adequats per a les funcions per a les que estan considerades.

Treball realitzat
S'avalua les mesures de seguretat existents abans, durant i després de la contractació, incloent l'existència d'acords de confidencialitat, conscienciació, etc.

Observació
És verifica l'existència d'acords de confidencialitat abans de l'inici d'un servei extern. És verifica l'existència del procediment de conscienciació, enviat a cada proveïdor extern abans dels seus serveis

Evidencies
És detallen les evidencies recollides: ▪ **EV005:** Recopilació d'acord de confidencialitats firmats amb anterioritat a l'inici del servei ▪ **EV006:** Procediment de conscienciació.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	7. La seguretat dels recursos humans	Conclusió	Conforme

Control ISO/IEC 27002:2013: 7.2 Durant l'ocupació
Garantir que els empleats i contractistes són conscients de les seves responsabilitats i compleixin seguretat de la informació

Treball realitzat
S'avalua les mesures de seguretat existents.

Observació
És detecta jornades inicials on es realitzen sessions sobre la conscienciació a la seguretat de la informació.

Evidencies
És detallen les evidencies recollides: ▪ **EV007:** Actes amb firmes dels presents en la jornada de conscienciació ▪ **EV008:** Documents repartits durant aquesta sessió.

Recomanació

No es detecta cap tipus d'enquesta per saber el nivell de conscienciació de cada proveïdor abans de donar el seu servei.

Estat	--	Responsable	--	Termini	--

Àrea	**7. La seguretat dels recursos humans**	Conclusió	Conforme

Control ISO/IEC 27002:2013: 7.3 Terminació i canvi d'ocupació
Per protegir els interessos de l'organització com a part del procés de canviar o acabar la feina.

Treball realitzat
S'avalua les mesures de seguretat després de la contractació.

Observació
S'observa que hi ha procediment de devolució dels materials, on es signa el dia de la seva sortida que no ha s'endu cap tipus d'informació

Evidencies
És detallen les evidencies recollides: ▪ **EV009:** Procediment de baixes. ▪ **EV010:** Documents de devolució de materials signats.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	8. Gestió d'actius	Conclusió	Conforme

Control ISO/IEC 27002:2013: 8.1 La responsabilitat dels actius
Identificar els actius de l'organització i definir les responsabilitats de protecció adequats

Treball realitzat
Es revisa que hi hagi un inventari dels actius que tracten o emmagatzemen informació corporativa.

Observació
És revisa alguns actius al atzar de l'organització, es revisa que tingui definit un propietari.

Evidencies
És detallen les evidencies recollides: ▪ **EV011:** Extracció d'actius a l'atzar de la CMDB.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	8. Gestió d'actius	Conclusió	Conforme

Control ISO/IEC 27002:2013: 8.2 Classificació de la Informació
Garantir que la informació rebi un nivell adequat de protecció d'acord amb la seva importància per a l'organització.

Treball realitzat
Es revisa la classificació de la informació i s'estableixin mesures de seguretat per a la gestió de suports.

Observació
S'observa els actius identificats amb dades confidencials, perfectament indicats a la CMDB. S'observa els últims informes de compliment normatiu d'aquest actius i el seu nivell de protecció.

Evidencies
És detallen les evidencies recollides: ▪ **EV011:** Extracció d'actius a l'atzar de la CMDB.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	8. Gestió d'actius	Conclusió	Conforme

Control ISO/IEC 27002:2013: 8.3 Mitjans de manipulació
Per evitar la divulgació no autoritzada, modificació, eliminació o destrucció de la informació emmagatzemada en els mitjans de comunicació.

Treball realitzat
És revisa que únicament el propietari de cada actiu té permisos de modificació, creació i eliminació, a més ell és responsable de mantenir la informació vigent.

Observació
En els projectes de creació de nous actius hauria d'existir l'estat de pendent d'integració.

Evidencies
És detallen les evidencies recollides: ▪ **EV011:** Extracció d'actius a l'atzar de la CMDB. ▪ **EV012:** Gestió d'altes i baixes a la CMDB.

Recomanació
És recomana incloure l'estat pendent d'integració, per tal de tenir identificat el nou actiu encara que no doni servei.

Estat	--	Responsable	--	Termini	--

Àrea	9. Control d'accés	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 9.1 Els requisits de negoci de control d'accés
Per limitar l'accés a les instal·lacions de processament d'informació.

Treball realitzat
És revisa el procediment d'accessos de visites i d'externs, el registre d'entrada i sortida i el mètode per accedir.

Observació
En els diferents edificis es detecta que espot accedir per diferents zones sense identificació. Per accedir als edificis on es troba el CPD si que es obligatori accedir per un torn, però es pot passar la mateixa targeta identificadora múltiples vegades.

Evidencies
És detallen les evidencies recollides: ▪ **EV013:** Procediment d'accés de visites/personal extern ▪ **EV014:** Registre d'entrada i sortida**.**

Recomanació
Definir un accés on sigui obligatori la presentació de la targeta identificadora.

Estat	Pendent	Responsable	Joan D.	Termini	6 mesos

Àrea	9. Control d'accés	Conclusió	Conforme

Control ISO/IEC 27002:2013: 9.2 Gestió d'accés dels usuaris
Garantir l'accés d'usuaris autoritzats i per evitar l'accés no autoritzat als sistemes i serveis

Treball realitzat
S'observa la gestió d'altes i baixes dels usuaris dels sistemes a traves del IDM i del AD.

Observació
És verifica els control d'accessos als sistemes, i els controls de verificació realitzats a través del SIEM.

Evidencies
És detallen les evidencies recollides: ▪ **EV015:** Procediment d'accés lògic ▪ **EV016:** Gestió d'altes i baixes

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	9. Control d'accés	Conclusió	Conforme

Control ISO/IEC 27002:2013: 9.3 Responsabilitat dels usuaris
Fer que els usuaris responsables de salvaguardar la informació d'accés.

Treball realitzat
S'observa la gestió d'usuaris privilegiats i altres de servei, responsables de mantenir aquesta informació els responsables en l'eina PMP.

Observació
És verifica els control d'accessos als sistemes, i els controls de verificació realitzats a través del SIEM.

Evidencies
És detallen les evidencies recollides: ▪ **EV015:** Procediment d'accés lògic ▪ **EV016:** Gestió d'altes i baixes

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	9. Control d'accés	Conclusió	Conforme

Control ISO/IEC 27002:2013: 9.4 Sistema de control i d'accés a les aplicacions
Per prevenir l'accés no autoritzat a sistemes i aplicacions.

Treball realitzat
És revisen els diferents events generats al SIEM per aquest tipus de control. És revisa el registre de consultes realitzada a diferents usuaris amb privilegis en el PMP.

Observació
És verifica els control d'accessos als sistemes, i els controls de verificació realitzats a través del SIEM. També es verifica l'ús d'usuaris privilegiats queda registrat qui consulta aquesta informació en el PMP.

Evidencies
És detallen les evidencies recollides: ▪ **EV017:** Gestió d'alertes SIEM ▪ **EV018:** Gestió d'usuaris PMP

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	10 Criptografia	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 10.1 controls criptogràfics
Per garantir l'ús adequat i eficaç de la criptografia per protegir la confidencialitat, autenticitat i/o integritat de la informació.

Treball realitzat
Es realitzen controls bàsics sobre certificats digitals i claus criptogràfiques basats principalment en la bona voluntat de les persones implicades i en la repetició de les tasques, no estant documentats.

Observació
És detecta que no hi ha una política definida sobre l'ús i el manteniment de certificats digitals corporatius i claus criptogràfiques.

Evidencies
És detallen les evidencies recollides: ▪ **EV019:** Document amb llista de persones autoritzades a utilitzar els certificats digitals Corporatius. ▪ **EV020:** Llista de Certificats Digitals Corporatius en vigor.

Recomanació
--

Estat	Pendent	Responsable	David LL.	Termini	6 mesos

Àrea	**11.La seguretat física i ambiental**	Conclusió	Conforme

Control ISO/IEC 27002:2013: 11.1 Les àrees segures
Prevenir l'accés no autoritzat física, dany i interferència a les instal·lacions de processament d'informació i la informació de l'organització.

Treball realitzat
Es revisen les mesures de seguretat existents en l'accés físic a les instal·lacions i en especial a les zones més crítiques com el Centre de Procés de Dades (CPD) o l'arxiu.

Observació
Es verificar que el CPD disposa de mesures que garanteixin la integritat física dels sistemes d'informació (climatització, detecció i extinció d'incendis, subministrament elèctric de suport,

etc.)

Evidencies
És detallen les evidencies recollides: ▪ **EV021:** Projecte 2016 del nou CPD i els seus requeriments

Recomanació
--

Estat	--	**Responsable**	--	**Termini**	--

Àrea	**11.La seguretat física i ambiental**	**Conclusió**	No Conforme

Control ISO/IEC 27002:2013: 11.2 Equip
Per evitar la pèrdua, dany, robatori o el compromís dels actius i la interrupció de les operacions de l'organització.

Treball realitzat
Es revisa la seguretat física dels llocs del treball e inclús de l'antic CPD.

Observació
L'antic CPD no disposa de les mesures de seguretat, encara té actius que donen un dels principals serveis dels centres de donació.

Evidencies
És detallen les evidencies recollides: ▪ **EV022:** Anàlisis de riscos

Recomanació
--

Estat	Pendent	**Responsable**	Joan D.	**Termini**	6 mesos

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.1 Procediments i responsabilitats operacionals
Per garantir operacions correctes i segures d'instal·lacions de processament d'informació.

Treball realitzat
És realitza l'entrevista amb el responsable de Seguretat IT, indintificants els responsables de cada servei.

Observació
S'observa a la política els rols de cadascú definits i les seves responsabilitats.

Evidencies
És detallen les evidencies recollides: ▪ **EV023:** Política de seguretat, rols i responsabilitats

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.2 Protecció contra el malware
Garantir que les instal·lacions de processament d'informació i la informació estan protegits contra el malware.

Treball realitzat
S'entrevisten els administradors del antivirus a més del responsable del ATD en seguretat. És revisen els procediments i una activitat pràctica del funcionament del ATD.

Observació

S'observa que tot el phising es filtrat per l'antivirus, a més a més el ATD compta amb una amplia BBDD de coneixement pels casos que l'antivirus no actiu.

Evidencies
És detallen les evidencies recollides: ▪ **EV024:** Gestió del antivirus en Traun ▪ **EV025:** Procediment del ATD.

Recomanació
--

Estat	--	**Responsable**	--	**Termini**	--

Àrea	**12.Operacions de Seguretat**	**Conclusió**	Conforme

Control ISO/IEC 27002:2013: 12.3 Còpia de seguretat
Per evitar la pèrdua de dades.

Treball realitzat
És realitza entrevista amb el responsable de backup on es detalla cada acció del procediment. És tria varies mostres a examinar l'estat de l'últim backup.

Observació
Es verifica que coincideix amb els backups que s'han de realitzar.

Evidencies
És detallen les evidencies recollides: ▪ **EV026:** Procediment de gestió de backups

Recomanació
--

Estat	--	**Responsable**	--	**Termini**	--

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.4 Registre i supervisió
Per registrar els esdeveniments i generar evidència.

Treball realitzat
És revisen els procediments a seguir en quant a la detecció d'alertes, es revisen els KPI reportats mensualment d'aquestes alertes i s'extrau un excel amb les alertes registrades en l'eina de ticketing.

Observació
S'observa que cada alerta generada esta automatitzada amb l'eina de ticketing, d'aquesta manera es registra tots els events.

Evidencies
És detallen les evidencies recollides: ▪ **EV027:** Gestió d'alertes IPS ▪ **EV028:** Gestió d'alertes SIEM ▪ **EV029:** KPI de seguretat

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.5 de control de programari operacional
Per garantir la integritat dels sistemes operatius.

Treball realitzat
S'entrevista els desenvolupadors i als administradors.

Observació
Un cop es desplega el nou software s'han d'encarregar de tindré validat per la gent de Seguretat, aquestos realitzen un control de la versió de software i de programari maliciós.

Evidencies
És detallen les evidencies recollides: ▪ **EV030:** Procediment de gestió de vulnerabilitats. ▪ **EV031:** Sol·licitud d'instal·lació de software.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.6 La gestió tècnica de la vulnerabilitat
Prevenir l'explotació de vulnerabilitats tècniques

Treball realitzat
S'entrevista la persona responsable del procés i el responsable de riscos. És revisa el fluxe del procediment i la generació de scans de vulnerabilitats

Observació
S'observa que per cada scan de vulnerabilitats es genera un change en l'eina de ticketing, per a la correcció de vulnerabilitats es generen change i es reporten a l'eina de gestió de scans i vulnerabilitats Qualys, es realitza un extracte de les remediacions.

Evidencies
És detallen les evidencies recollides: ▪ **EV030:** Procediment de gestió de vulnerabilitats. ▪ **EV032:** Procés de remediació de vulnerabilitats.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	12.Operacions de Seguretat	Conclusió	Conforme

Control ISO/IEC 27002:2013: 12.7 Sistemes d'informació consideracions d'auditoria
Per minimitzar l'impacte de les activitats d'auditoria en els sistemes operatius.

Treball realitzat
S'entrevista el responsable del procés i els controls a revisar per a cada,els KPI mensuals, i l'extracció d'auditories de Qualys

Observació
Tot es gestiona a través del Qualys, on es pot analitzar totes les auditories realitzades y els seus resultats.

Evidencies
És detallen les evidencies recollides: ▪ **EV033:** Procediment de Policy Compliance ▪ **EV034:** Diferents guies de hardening

Recomanació

Estat	--	Responsable	--	Termini	--

Àrea	13. Seguretat de les comunicacions	Conclusió	Conforme

Control ISO/IEC 27002:2013: 13.1 de gestió de seguretat de xarxa
Per garantir la protecció de la informació en xarxes i les seves instal·lacions de suport de processament d'informació.

Treball realitzat

S'entrevista el responsable de l'àrea, és revisen els procediments i els contractes externs.

Observació

Es verifica tant l'existència de mecanismes per garantir la seva seguretat (sistemes tallafocs, sistemes IPS), com la seva correcta implantació i configuració.

Evidencies

És detallen les evidencies recollides:

- **EV035:** Contractes de diferents proveïdors de serveis en xarxa**.**
- **EV036:** Procediment de gestió de xarxes.

Recomanació

--

Estat	--	Responsable	--	Termini	--

Àrea	**13. Seguretat de les comunicacions**	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 13.2 La transferència d'informació

Per mantenir la seguretat de la informació transferida d'una organització i amb qualsevol.

Treball realitzat

És detalla la feina realitzada en aquesta area concreta.

Observació

No es realitza una revisió adequada dels logs, i tampoc estan configurats tots els equips de xarxa per reportar esdeveniments que permetin detectar accions que puguin afectar la seguretat de la informació.
Els contractes amb els proveïdors de serveis en xarxa enuncien les mesures de seguretat aplicables però no es concreten aquestes mesures i tampoc hi ha clàusules específiques sobre els mecanismes de supervisió i auditoria d'aquestes mesures.

Evidencies

És detallen les evidencies recollides:

- **EV035:** Contractes de diferents proveïdors de serveis en xarxa**.**

Recomanació

Establir procediments de generació i revisió de logs per a tots els equips de xarxa, de manera que permetin detectar errors o activitats maliciosa

Estat	Pendent	Responsable	David R.	Termini	6 mesos

Àrea	**14.Sistema d'adquisició, desenvolupament i manteniment**	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.1 Els requisits de seguretat dels sistemes d'informació
Garantir que la seguretat informàtica és una part integral dels sistemes d'informació a través de tot el cicle de vida. Això també inclou els requisits per als sistemes d'informació que proporcionen els serveis a través de xarxes públiques.

Treball realitzat
S'entrevista als responsables del WAF, els procediments i les remediacions que duen a terme.

Observació
Tots els sistemes i les URL publiques es troben darrera del WAF (web application firewall), tota la seguretat es gestiona a través de ells.

Evidencies
És detallen les evidencies recollides: ▪ **EV037:** Contractes de diferents proveïdors de serveis en xarxa**.** ▪ **EV033:** Procediment de Policy Compliance ▪ **EV034:** Diferents guies de hardening ▪ **EV038:** Procediment de gestió del WAF

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	14.Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.2 Seguretat en els processos de desenvolupament i suport
Per assegurar que la seguretat d'informació es dissenya i implementa dins el cicle de vida de desenvolupament de sistemes d'informació.

Treball realitzat
S'entrevista l'analista en seguretat qui representa totes les reunions de nous desenvolupaments, on s'han de verificar amb les eines de seguretat.

Observació
S'observa els fluxe de nous projectes la implicació i la verificació per part de seguretat, a cada tasca realitzada hi ha adjunt els informes d'aprovació des de Seguretat.

Evidencies
És detallen les evidencies recollides: ▪ **EV037:** Contractes de diferents proveïdors de serveis en xarxa**.** ▪ **EV033:** Procediment de Policy Compliance ▪ **EV034:** Diferents guies de hardening ▪ **EV038:** Procediment de gestió del WAF

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	14.Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.3 Les dades de prova
Garantir la protecció de dades que s'utilitza per a les proves

Treball realitzat
S'entrevista l'analista de riscos, tots aquells entorns no productius s'emmascaren les dades, Traun disposa de l'eina adequada i desplegada als altres departaments.

Observació
S'analitzen alguns entorns de preproducció i desenvolupament on s'emmascaren les dades.

Evidencies
És detallen les evidencies recollides: ▪ **EV037:** Contractes de diferents proveïdors de serveis en xarxa. ▪ **EV033:** Procediment de Policy Compliance ▪ **EV034:** Diferents guies de hardening ▪ **EV038:** Procediment de gestió del WAF

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	15.Les relacions amb proveïdors	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 15.1 Seguretat de la informació en relació amb els proveïdors
Garantir la protecció dels actius de l'organització que sigui accessible pels proveïdors.

Treball realitzat
Es revisen la subcontratació de serveis i l'externalització de recursos, a cada depertament el 70% del personal es extern i té el mateix perfil i accessos que una persona interna. Es revisa el material utilitzat per aquest personal.

Observació
És detecta que personal extern diposa del seu propi material sense les securitacions de Traun Proveïdors externs tenen els mateix permisos que els interns donant el 100% d'informació dels actius.

Evidencies
És detallen les evidencies recollides: ▪ **EV039:** Acords de confidencialitat ▪ **EV40:** Documentació de prestació de serveis.

Recomanació
Qualsevol dispositiu connectat a la xarxa interna ha de complir els requeriments de seguretat, per tant recomanem que se'ls hi doni o es securitzi els dispositius de proveïdors externs.

Estat	En curs	Responsable	Nuria B.	Termini	6 mesos

Àrea	**15.Les relacions amb proveïdors**	Conclusió	Conforme

Control ISO/IEC 27002:2013: 15.2 La gestió de la prestació de serveis de proveïdors
Mantenir un nivell acordat de seguretat de la informació i la prestació de serveis en línia amb els acords amb proveïdors.

Treball realitzat
S' ha comprovat els aspectes contractuals en la contractació de tercers (acords de confidencialitat, acords de nivell de servei, etc.), així com el seguiment existent sobre els serveis prestats per aquests

Observació
Des de l'àrea de RRHH es gestionen tota la documentació necessària abans de la prestació de servei, sense aquest requeriments l'empresa no té accés a les instal·lacions.

Evidencies
És detallen les evidencies recollides: ▪ **EV039:** Acords de confidencialitat ▪ **EV40:** Documentació de prestació de serveis.

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	16.Gestió d'incidents de seguretat d'informació	Conclusió	No Conforme

Control ISO/IEC 27002:2013: 16.1 Gestió dels incidents de seguretat de la informació i millores
Per garantir un enfocament coherent i eficaç per a la gestió d'incidents de seguretat de la informació, incloent-hi la comunicació d'esdeveniments i debilitats de seguretat.

Treball realitzat
Revisió del procediment i fluxe de la gestió d'incidents de Traun.

Observació
No es detecta un procediment com a tal ni els resursos necessaris per a gestionar-ho.

Evidencies
És detallen les evidencies recollides: ▪ **EV027:** Gestió d'alertes IPS ▪ **EV028:** Gestió d'alertes SIEM

Recomanació
Subcontractació del servei.

Estat	En curs	Responsable	David LL.	Termini	4 mesos

Àrea	17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	Conclusió	Conforme

Control ISO/IEC 27002:2013: 17.1 La continuïtat seguretat de la informació
La continuïtat seguretat de la informació ha de formar part dels sistemes de gestió de continuïtat de negoci de l'organització.

Treball realitzat
Es revisa els plans de continuïtat de negoci per als sistemes d'informació de l'organització.

Observació
És verifica que els plans són revisats i provats periòdicament i el fluxe del procediment esta actualitzat i en vigor.

Evidencies
És detallen les evidencies recollides: ▪ **EV041:** Procediment de SCM ▪ **EV042**: Probes de PRD

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	**17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci**	Conclusió	Conforme

Control ISO/IEC 27002:2013: 17.2 Les redundàncies
Assegurar la disponibilitat d'instal·lacions de processament d'informació.

Treball realitzat
És revisen la documentació de les últimes probes de PRD i la periodicitat d'aquestes.

Observació
Traun disposa d'un pla anual de probes de PRD i amb pla d'accions.

Evidencies
És detallen les evidencies recollides: ▪ **EV041:** Procediment de SCM ▪ **EV042**: Probes de PRD

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	18.Compliment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 18.1 El compliment dels requisits legals i contractuals
Per evitar l'incompliment de les obligacions legals, estatutàries, reglamentàries o contractuals relacionades amb la seguretat de la informació i de qualssevol requisits de seguretat.

Treball realitzat
És revisen els tipus d'auditories internes i quines polítiques es revisem.

Observació
Traun compta amb una planificació d'auditoria interna per tal d'assegurar la seva integritat i confidencialitat dels seus actius.

Evidencies
És detallen les evidencies recollides: ▪ **EV40:** Documentació de prestació de serveis. ▪ **EV043:** Sistemes afectats per la LOPD

Recomanació
--

Estat	--	Responsable	--	Termini	--

Àrea	18.Compliment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 18.2 opinions seguretat de la informació
Garantir que la seguretat informàtica és implementat i operat d'acord amb les polítiques i procediments de l'organització.

Treball realitzat
És revisen els tipus d'auditories internes i quines polítiques es revisem.

Observació
Traun compta amb una planificació d'auditoria interna per tal d'assegurar que es compleixen

ambles polítiques establertes.

Evidencies
És detallen les evidencies recollides: ▪ **EV40:** Documentació de prestació de serveis. ▪ **EV043:** Sistemes afectats per la LOPD ▪ **EV044:** Documentació Comitè de Seguretat

Recomanació
--

Estat	--	**Responsable**	--	**Termini**	--

8. Resultats de l'auditoria

L'auditoria s'ha realitzat una sèrie d'entrevistes, visites i proves per avaluar el grau de maduresa de les mesures de seguretat implantades pel que fa als diferents dominis i objectius de control de la Norma ISO/IEC 27002: 2013.

El grau de maduresa en què es troben els diferents dominis ha passat d'una mitjana de "L2 i L3" a una mitjana actual de "L4 i L5" segons els nivells de maduresa utilitzats, CMM.

L'evolució d'aquesta maduresa podem veure reflectida en la següent taula:

Àrees	CMM 2016	CMM 2019
5. Polítiques de la Seguretat de la Informació	L5	L5
6.Organització de la seguretat de la informació	L3	L4
7. La seguretat dels recursos humans	L2	L5
8. Gestió d'actius	L2	L5
9. Control d'accés	L3	L4
10.Criptografia	L0	L2
11.La seguretat física i ambiental	L3	L4
12.Operacions de Seguretat	L5	L5
13.Seguretat de les comunicacions	L4	L4
14.Sistema d'adquisició, desenvolupament i manteniment	L3	L5
15.Les relacions amb proveïdors	L4	L4
16.Gestió d'incidents de seguretat d'informació	L0	L2
17.Aspectes de seguretat d'informació de gestió de la continuïtat del negoci	L5	L5
18.Compliment	L2	L4

Com a resultat de l'anàlisi de cada un dels controls de la ISO27002 de referència s'han trobat un total de 7 "No Conformitats" que hauran de ser corregides.

Aquestes "No Conformitats" es troben en els següents controls de la norma:

- 6.2 Els dispositius mòbils i el teletreball
- 9.1 Els requisits de negoci de control d'accés
- 10.1 Controls criptogràfics
- 11.2 Equip
- 13.2 La transferència d'informació
- 15.1 Seguretat de la informació en relació amb els proveïdors
- 16.1 Gestió dels incidents de seguretat de la informació i millores