Pla director de seguretat de la informació

Nom Estudiant: David González Mas

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

Nom Consultor: Arsenio Tortajada Gallego

Data Lliurament: 04/01/2017


Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

FITXA DEL TREBALL FINAL

Títol del treball:	*Pla director de seguretat de la informació*
Nom de l'autor:	*David González Mas*
Nom del consultor:	*Arsenio Tortajada Gallego*
Data de lliurament (mm/aaaa):	*01/2017*
Àrea del Treball Final:	*Sistemes de gestió de seguretat de la informació*
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

L'objecte del present treball consisteix en l'elaboració d'un pla director de seguretat de la informació per la Autoritat Portuària de Zapata. Aquesta organització, de caràcter públic, que ofereix serveis a la cadena logística, per requeriments legals i motius històrics està fortament sensibilitzada amb la implantació de mesures físiques a les seves instal·lacions, però que tot just inicia el procés per assegurar els seus actius d'informació.

Per a dur a terme aquest procés, que s'ha dividit en 5 fases, s'ha agafat com a referència la normativa ISO/IEC 27001:2013

Fase 1: Anàlisi i descripció de l'Autoritat Portuària de Zapata. Durant aquesta fase s'ha dut a terme un anàlisi de compliment inicial prenent com a referencia la norma ISO 27002.

Fase 2: Elaboració d'un sistema de gestió documental, amb el cos documental bàsic d'un SGSI: política de seguretat, procediment de revisió. Procediment d'auditories internes, SOA, gestió d'indicadors, metodologia d'anàlisi de riscos aplicada, rols i responsabilitats.

Fase 3: Elaboració d'un anàlisi de riscs basant-nos en la metodologia MAGERIT v3

Fase 4: Proposta d'un conjunt de projectes per mitigar els riscos detectats en la fase 3 i aconseguir un millor grau d'acompliment per a una futura auditoria de certificació ISO/IEC 27001:2013.

Fase 5: En aquesta fase s'ha calculat la evolució de l'organització objecte de l'estudi en quant a l'evolució en el grau d'acompliment en la norma ISO 27002, prenent com a punt inicial la Fase 1 i com a final la implantació dels projectes proposats a la fase 4.

Abstract (in English, 250 words or less):

The purpose of this work is the development of a master plan for information security for the Port Authority of Zapata. This organization, a public body that offers services to the supply chain, has implemented a number of physical security measures in its facilities, but that just starts the process to ensure their information assets.

To carry out this process, which has been divided into five phases, the ISO / IEC 27001: 2013 normative has been taken as a reference.

Phase 1: Analysis and description of the Port Authority of Zapata. During this phase has conducted an initial analysis of compliance taking in account the ISO 27002 normative.

Phase 2: Development of a document management system, the basic body of a documentary ISMS: security policy, review procedure, procedure for internal audits, SOA, management indicators, risk analysis methodology applied, roles and responsibilities.

Phase 3: Preparation of a risk analysis based on the methodology MAGERIT v3

Phase 4: Proposal of a set of projects to mitigate the risks identified in phase 3 and achieve a better level of compliance for a future audit of ISO / IEC 27001: 2013.

Phase 5: At this stage we have calculated the evolution of the organization under study and its degree of compliance in ISO 27002, taking as a starting point and a Phase 1 and taking in account the implementation of projects proposed in phase 4.

Paraules clau (entre 4 i 8):

seguretat, informació, 27001, 27002, pla director, anàlisi de riscos, auditoria.

Índex

1. Introducció

1.1. Context i justificació del Treball

Aquest treball de final de màster consisteix en la realització d'un pla director de seguretat de la informació per a una organització de caràcter públic, sensibilitzada i acostumada a establir mesures físiques de seguretat en les seves instal·lacions i els seus processos, però que tot just dona les primeres passes en matèria de protecció dels seus actius d'informació.

1.2. Objectius del Treball

- Elaboració d'un pla director per l'Autoritat Portuària de Zapata.
- Identificar els riscos als que s'exposen els actius d'informació de l'organització.
- Identificar l'eficiència dels controls de seguretat actualment implementats.
- Establir els controls de seguretat adequats segons el grau de protecció requerit.
- Utilitzar el pla director per crear consciència i formalitzar el procediment de seguretat de la informació en la organització.
- Identificar el grau de maduresa de l'organització en quant a seguretat de la informació per plantejar-se afrontar una certificació ISO/IEC 27001.

1.3. Enfocament i mètode seguit

Per realitzar aquest treball d'una forma ordenada i poder obtenir resultats i conclusions de cadascuna de les tasques que composen el pla director de seguretat, s'han seguit una sèries de fases, amb els objectius de cada fase proposats pel tutor de l'assignatura i amb l'obtenció de resultats de cadascuna de les fases.

Per a obtenir informació i poder completar cadascuna de les fases s'ha recopilat informació de l'empresa: la seva memòria, llistat d'actius controlats per sistemes d'informació, documentació obtinguda de repositoris corporatius (intranet i recursos humans). S'han mantingut també breus entrevistes amb els responsables de negoci per determinar el grau de criticitat i impacte dels actius dels quals són responsables.

1.4. Breu sumari de productes obtinguts

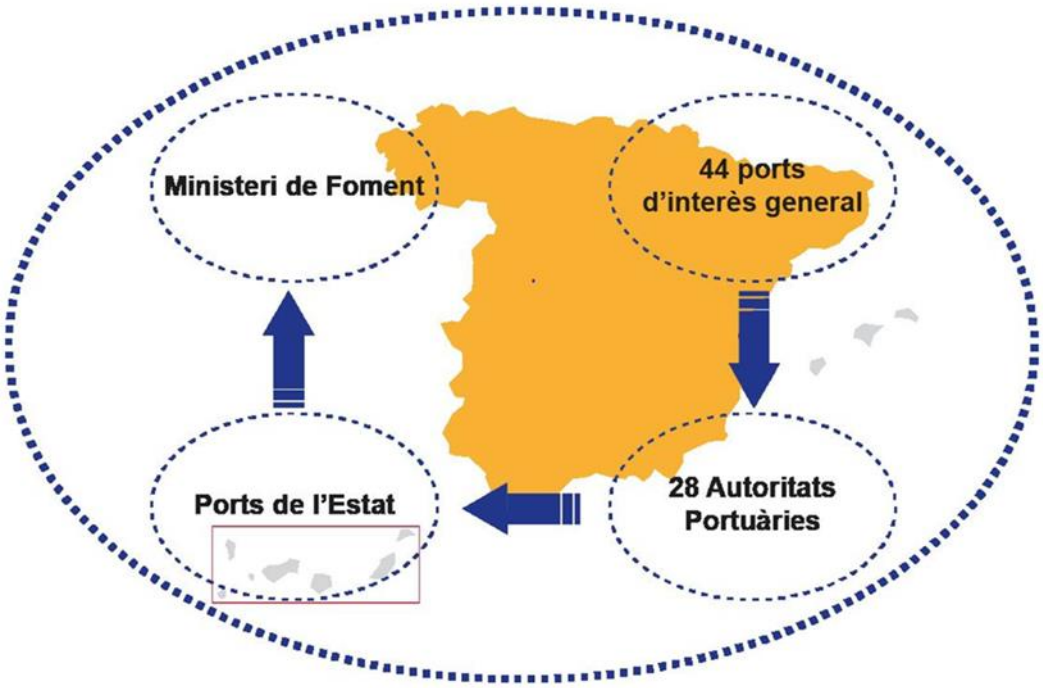
Fase	Descripció	Capítol
Fase 1	Descripció de l'organització seleccionada, establiment d'objectius per al pla director. Anàlisi diferencial prenent com a referència la norma ISO 27002.	**2,3,4**
Fase 2	Elaboració del cos documental del SGSI.	5
Fase 3	Elaboració d'un anàlisi de riscos. Identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.	6
Fase 4	Proposta de projectes per alinear-se amb el PDSI i pal·liar els riscos identificats en la Fase 3.	7
Fase 5	Avaluació de controls, maduresa i nivell de compliment.	8
Fase 6	Consolidació dels resultats obtinguts durant el procés d'anàlisis. Realització dels informes i presentació executiva a Direcció. Entrega del projecte final.	

Taula 1-sumari de productes obtinguts

2. L'Autoritat Portuària de Zapata

2.1. Qui és l'Autoritat Portuària de Zapata?

L'Autoritat Portuària de Zapata (APZ), és un organisme de dret públic amb personalitat jurídica i patrimoni propis. Té plena capacitat d'obrar per al desenvolupament de les seves finalitat i actua amb subjecció a l'ordenament jurídic privat excepte en l'exercici de les funcions de poder públic que l'ordenament li atribueix. Es regeix per les disposicions de la Llei d'organització i funcionament general de l'Estat i per la seva gestió específica mitjançant el RDL 2/2011, que aprova el text refós de la Llei de Ports de l'Estat i la marina mercant. L'APZ forma part del Sistema Portuari Espanyol, que està format per 44 ports d'interès general, integrats en un total de 28 autoritat portuàries, que depenen de l'organisme públic Ports de l'Estat i que alhora depèn del Ministeri de Foment del Govern d'Espanya.



Il·lustració 1-sistema portuari estatal

Les principals funcions i competències de l'APZ són:

Els serveis que presta l'APZ als usuaris del Port de Zapata són els següents:

- Serveis generals: Ordenació, coordinació i control de tràfic marítim, servei de policia, prevenció i control d'emergències, enllumenat, neteja...
- Serveis portuaris: Tècnic-nàutics(practicatge, remolc i amarratge).
- Serveis de senyalització marítima: Manteniment i conservació de fars i senyals marítims de la zona assignada.
- Serveis comercials: Prestació de serveis de naturalesa comercial vinculats a l'activitat portuària.
- Gestió, dinamització i explotació d'infraestructures i obres portuàries.

2.2. La cultura organitzativa

Missió

Contribuir al desenvolupament econòmic i social del seu Hinterland (àrea d'influència) de forma sostenible, en un context de màxima competitivitat. Impulsar la modernització i l'adequació de les infraestructures portuàries a la prestació de serveis de valor afegit, sota un marc de cohesió entre els membre de la comunitat portuària.

Visió

- Consolidar el lideratge al sistema portuària en tràfics de líquids a doll i sòlids a lloure.
- Desenvolupar l'estratègia per ser port logístic de referència, impulsor del pool logístic del sud-oest europeu.
- Ser una referencia intermodal d'integració als programes d'autopistes del mar.
- Ser reconeguda per la seva importància en l'activitat econòmica del seu Hinterland.

Valors

- Lideratge.
- Integritat de criteris.
- Responsabilitat social corporativa.
- Equip humà eficient i compromès.
- Transparència.
- Orientació al client.
- Excel·lència operativa.
- Innovació tecnològica i de gestió.
- Desenvolupaments sostenible.

2.3. Situació

El Port de Zapata gaudeix d'una situació geo estratègica privilegiada, en un indret on conflueixen diverses grans infraestructures viàries i ferroviàries bàsiques. Al mateix temps, el fet d'estar ben dimensionat i comptar amb unes excel·lents instal·lacions fan que l'APZ sigui un dels ports més importants de la Península Ibérica.

2.4. Accessibilitat

L'accés viari al Port de Zapata està garantit per l'Eix Transversal i les entrades del moll de llevant. Aquests accessos estan connectats a una xarxa formada per les principals autopistes, autovies i carreteres. Així mateix el Port de Zapata disposa d'una xarxa interior ferroviària que permet que el tren arribi a tots els molls i esplanades.

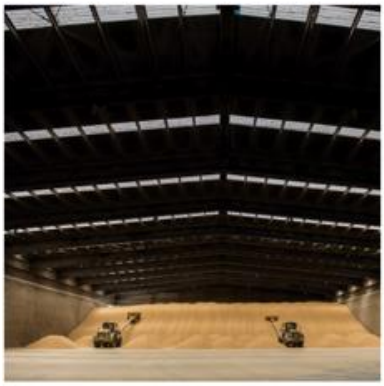
2.5. Característiques tècniques

El Port de Zapata compta amb una superfície terrestre de 543 ha i 18000 ha de làmina d'aigua. Un canal d'entrada de 450 metres d'amplada i una línia d'atracada de 17 km.

2.6. Tràfics

El Port de Zapata, en volum total de mercaderies, és un dels ports més importants de l'Estat espanyol.

- Sòlids a lloure: són bàsicament productes agroalimentaris, carbons i minerals. Els primers són descarregats en sitges, mentre que els dos darrers són apilats als molls.



Il·lustració 3-magatzem de gra

Il·lustració 2-cinta transportadora de carbó

- Líquids a doll: Són productes químics, petrolífers i els seus derivats.

Il·lustració 4-buc de transport químic

- Càrrega general: és tota aquella mercaderia no inclosa en el concepte de mercaderia a granel, des de matèries primeres fins a productes de consum. Pot ser càrrega contenitzada (en contenidors) o no contenitzada.

Il·lustració 6-ro-ro

Il·lustració 5-grues per contenidors

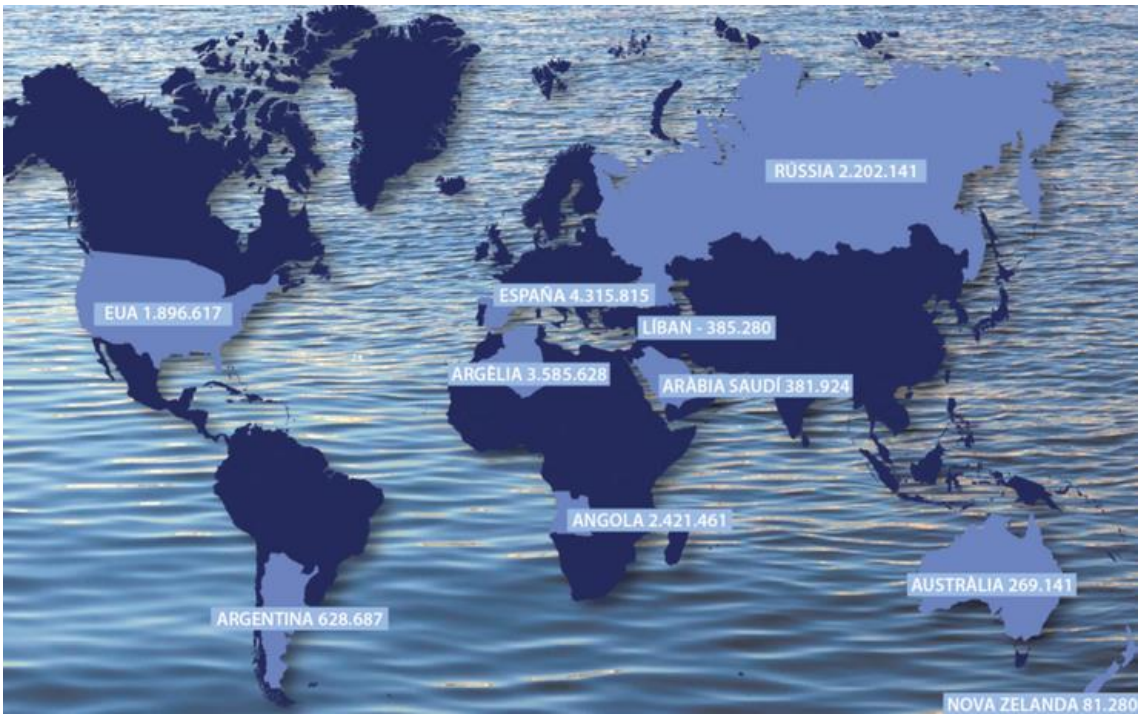
2.7. Nomenclatura dels molls i usos portuaris

Moll	Ús Portuari
Molls 1,2 i 3	Sòlids a lloure (principalment energètics)
Moll 4	Sòlids a lloure i mercaderia general
Moll 5	Mercaderia general convencional
Moll 6	Pesca
Moll 7	Fruita
Moll 8	Sòlids a lloure i mercaderia general
Moll 9	Productes petrolífers i químics
Moll 10	Mercaderia general en contenidor
Molls 11 i 12	Vehicles, mercaderia general, siderúrgics
Pantalà 1	Productes petrolífers
Pantalà 2	Productes petrolífers

Taula 2-noms de molls i usos portuaris

2.8. Internacionalització

El Port de Zapata està connectat pràcticament amb tot el món i compta amb un bon número de línies marítimes regulades que fan possible l'arribada de qualsevol tipus de mercaderia a qualsevol lloc del món i viceversa.

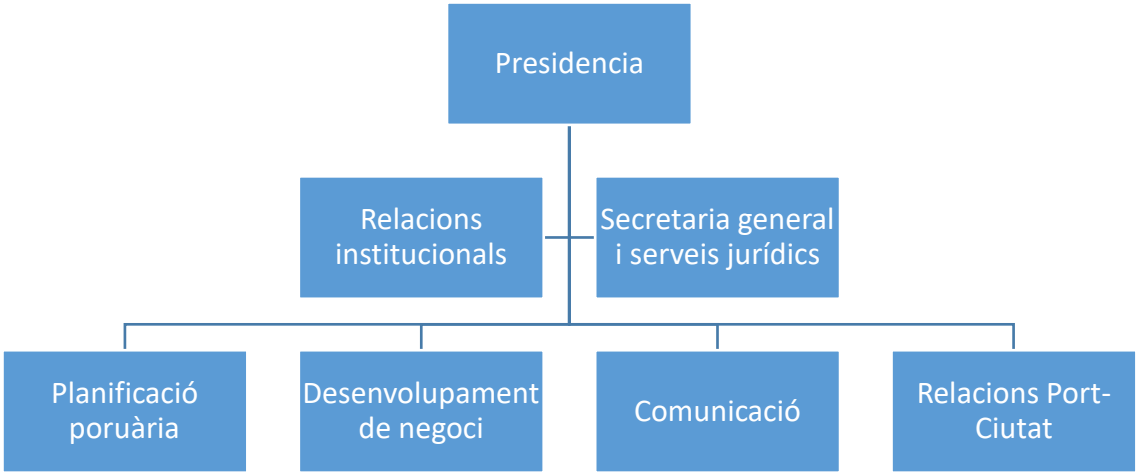


Il·lustració 7-Presencia internacional

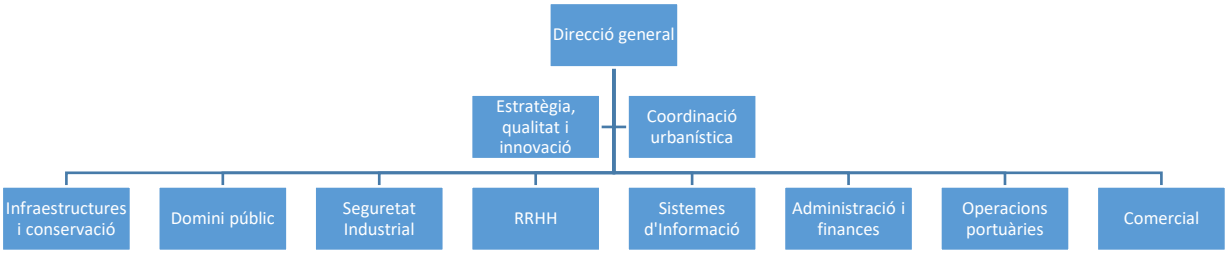
Tràfic total de mercaderies des del / fins al Port de Zapata en Tones.

2.9. El capital humà i l'estructura organitzativa

L'APZ compta a una estructura institucional depenent de la presidència, que és escollida pel govern autonòmic. El Director General és escollit pel President amb el vist i plau de l'òrgan supervisor Ports de l'Estat.



Il·lustració 8-Organigrama presidència



Il·lustració 10-Organigrama direcció

L'APZ està formada per una plantilla de 250 persones, 14 de les quals formen part dels òrgans de direcció.

Àrea d'activitat	Treballadors
Personal adscrit al servei de la Policia	55
Personal adscrit al servei de manteniment	7
Personal d'oficina adscrit al conveni col·lectiu	113
Personal d'oficina no adscrit al conveni col·lectiu	32
Personal adscrit al servei de bàscules	12
Personal adscrit al servei de guarda molls d'operacions	5
Personal adscrit al servei d'aigües	8
Personal adscrit al servei de control portuari	15
Personal adscrit a servei de senyals marítimes	2
Personal adscrit a vigilància d'obres	4

Taula 3-personal

2.10. El capital humà i l'estructura organitzativa

Pel que fa a les seus, tot el personal està dintre del recinte portuari. Tot i que no estan dintre del mateix edifici, el territori Portuari és gestionat per l'Autoritat Portuària i les xarxes de comunicacions són propietat d'aquesta. L'APZ té desplegada una xarxa de comunicacions que dóna cobertura a tot el recinte portuari, tant per veu, com per dades, videovigilància, alarmes i telemetria.
També existeix la possibilitat de treballar en mobilitat, sobretot el personal del departament comercial i el vinculat a la presidència. Aquests usuaris disposen de sistemes de processament d'informació portables (mòbils, tauletes, ordinadors portàtils).

Principals seus de l'APZ:

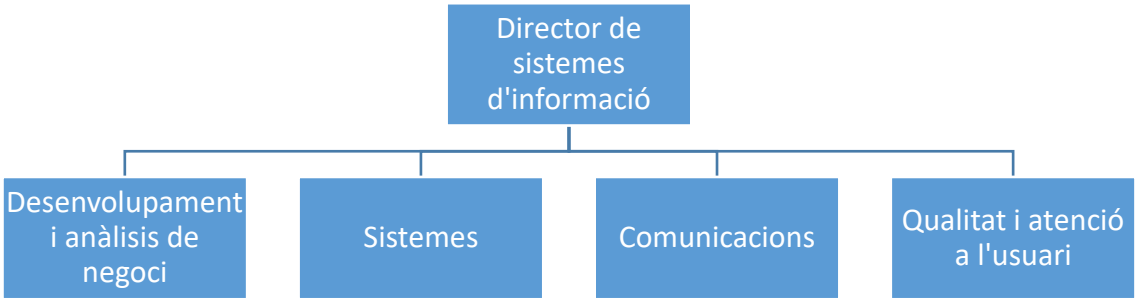
- Edifici d'oficines: Es tracta de la seu principal. Es on està ubicada la Presidència, Direcció, personal d'enginyeria, operacions, finances, sistemes d'informació, comunicació relacions institucionals, RRHH, domini públic, estratègia i qualitat. Es du a terme la majoria de tasques relacionades directament amb el negoci i les activitats de suport a aquestes.
- Edifici de la policia: Seu de la policia. Es du a terme el servei de policia i altres tasques de vigilància i protecció portuària.
- Edifici de control portuari: Es gestionen els serveis de tràfic portuari.
- Altres edificis de servei: aiguades, inspeccions, magatzems, sales tècniques, estacions transformadores.

2.11. El departament de seguretat industrial

El departament de seguretat industrial és, en última instància, el responsable de la seguretat integral de les operacions i d'altres activitats industrials i auxiliars de l'APZ. S'encarrega de l'elaboració dels plans de protecció i de vetllar pel compliment de la normativa vigent en matèria de seguretat.
De forma tradicional ha col·laborat amb d'altres departaments, especialment amb operacions i instal·lacions per implementar mesures de seguretat física per protegir les operacions dins del port.
El Port de Zapata compta amb unes mesures de seguretat física per sobre dels estàndards de mercat: tanques virtuals, sistema de càmeres amb detecció de moviment, radars, tanques sensoritzades.
El departament disposa d'un sistema de control avançat que permet integrar totes les senyals d'alarmes, tanques, imatges de càmeres i correlar events. Aquest sistema de control forma part del sistema global que utilitza el departament, juntament amb la policia, per a realitzar la gestió d'emergències.

Conscient de la importància que té, cada cop més, la seguretat de la informació en les organitzacions, el departament de seguretat industrial i el departament de sistemes d'informació han establert certs canals de col·laboració. En concret, estan treballant per poder integrar els elements de seguretat física dintre del SIEM de sistemes d'informació i poder rebre en el sistema de control avançat informació relativa a incidents de ciberseguretat en els dispositius físics.

2.12. El departament de sistemes d'informació



Il·lustració 11-Organigrama sistemes d'informació

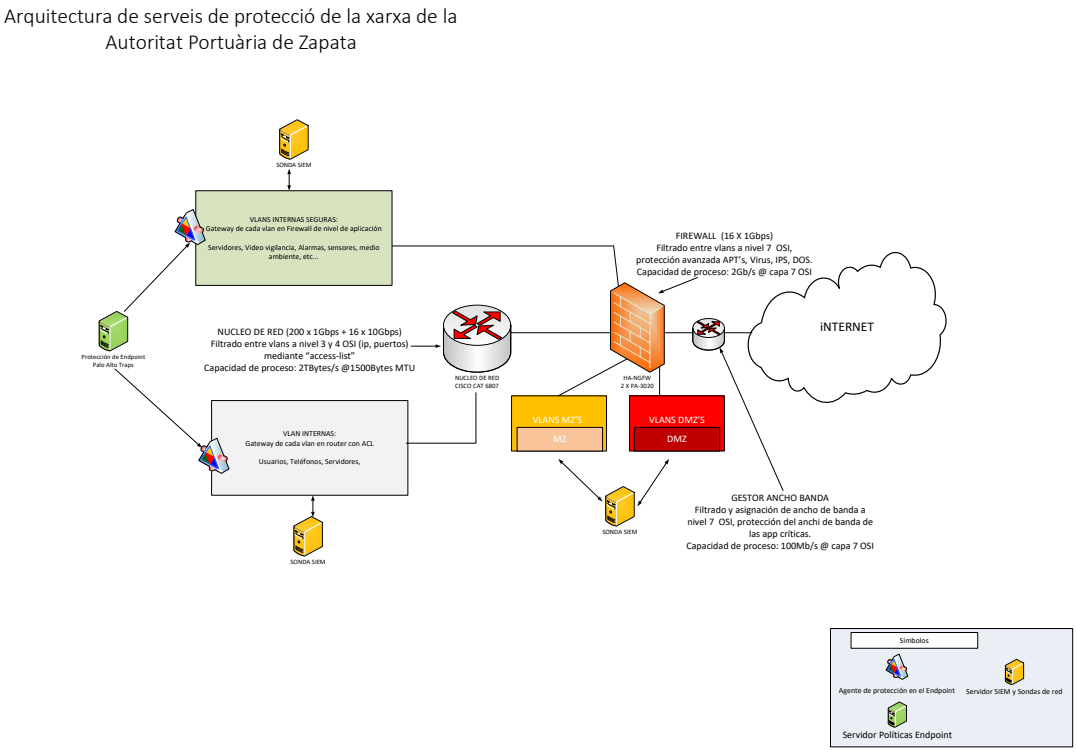
El departament de sistemes d'informació està format per un director, quatre responsables (comandaments mitjos del departament) i un pool de cinc tècnics que donen servei a les diferents línies de treball descrites en l'organigrama anterior.

El director de sistemes d'informació forma part del comitè executiu de l'organització i recentment ha estat nomenat responsable de seguretat de la informació. Tot i que no hi ha un suport formal a la seguretat de la informació per part dels òrgans de govern, el director de sistemes d'informació, a través d'un exercici de càlcul de l'impacte de la pèrdua d'actius d'informació, ha aconseguit despertar l'interès de la direcció en la seguretat de la informació i ha aconseguit una partida pressupostària per la realització del PDS i la implementació de les iniciatives quick-win que se'n puguin derivar.

El servei d'atenció a l'usuari dóna servei al client intern de l'organització i a l'extern en aquelles aplicacions que relacionen l'autoritat portuària amb la comunitat portuària (resta d'usuaris del Port de Zapata).

Els comandaments mitjos del departament són responsables del servei que tenen assignat (desenvolupament, sistemes, comunicacions i atenció a l'usuari). Gestionen la feina dels tècnics i gestionen els contractes de manteniment i/o nous projectes relacionats amb el servei del qual són responsables. El departament de sistemes d'informació dóna servei de comunicacions a tot el recinte portuari. Aquests departament, conscient de la importància de la securització dels serveis de xarxa, durant els últims anys ha realitzat un esforç important en redissenyar i fer més segura la seva infraestructura de

comunicacions. A continuació es pot veure un diagrama de serveis de seguretat de la xarxa de comunicacions:



Il·lustració 12-serveis de protecció de xarxa

L'Organització disposa d'un data center propi i diverses sales tècniques distribuïdes pel recinte portuari. Les sales tècniques tenen com a objectiu fer arribar la xarxa i els serveis de computació, dades i telefonia a tot el recinte portuari.

L'accés a aquest data center i a les sales tècniques disposa d'un control d'accessos independent del de la resta de la organització, gestionat directament pel departament de sistemes i amb coneixement per part del servei de policia del port. Aquest sistema de control d'accés registra les entrades i sortides del personal autoritzat a entrar en aquestes sales. A més, disposen de videovigilància, sensors de temperatura, humitat, foc i les seves respectives alarmes.

En el data center hi ha allotjats els sistemes de processament de la informació que donen suport als processos de negoci de l'organització i d'altres aplicacions auxiliars al negoci. Els serveis de computació, tant de les sales tècniques com del data center, són responsabilitat del departament de sistemes d'informació, mentre que el subministrament elèctric, refrigeració, vigilància i alarmes depenen d'altres departaments (principalment el departament d'infraestructures i conservació).

El sistema productiu (bases de dades, servidors d'aplicacions, servidors web) estan allotjats en un conjunt de virtualitzadors, redundats entre ells i dintre de la VLAN corresponent a servidors. De les màquines que corren en aquests virtualitzadors es realitza una còpia de seguretat diària incremental i una total setmanal. Es procedeix de la mateixa forma amb les dades d'aquestes màquines. La còpia de seguretat es fa a un sistema d'emmagatzematge dedicat. Posteriorment es còpia a dues cintes. Una de les cintes es conserva en el mateix data center i l'altra s'envia a una caixa de seguretat de una empresa especialitzada en continuïtat de negoci.
En el data center, a més, estan allotjats els cores de comunicacions de la xarxa de l'APZ i del recinte portuari. També està allotjat el sistema de telefonia. Es tracta d'un sistema de telefonia IP, redundat a nivell físic (actiu-passiu).
L'accés lògic a aquests sistemes (controladors de domini, servidors de correu, servidors de bases de dades, aplicacions, directori actiu, sistema de fitxers, controladors de xarxa) per part dels administradors del sistema està monitoritzat i auditat per un sistema específic.
Les sales tècniques serveixen bàsicament per allotjar la electrònica de distribució de la xarxa de comunicacions i actuen com a centres nodals i punts de repetició de la senyal. Tant les sales tècniques com el data center, disposen de sistemes d'alimentació ininterrompuda. El data center, a més, disposa d'un grup electrogen per garantir el subministrament elèctric.
El departament de sistemes d'informació és responsable del desenvolupament, manteniment i continuïtat dels següents sistemes que donen suport als processos de negoci:

- Port Community System (PCS): Es tracta d'un sistema de sol·licitud telemàtica de serveis portuaris. Els clients de l'APZ sol·liciten de forma telemàtica a l'APZ els serveis generals i tècnic-nàutics que aquesta gestiona. A més serveix perquè les empreses usuàries del port demanin serveis a altres administracions i serveis comercials a altres empreses usuàries del port. El PCS és una aplicació web (servidor web, servidor d'aplicacions, base de dades, web services) accessible a través d'internet.
- Integra II: Es tracta d'un sistema de gestió portuària. Un cop rebudes les sol·licituds a través del PCS, els tècnics del departament d'operacions portuàries gestionen les sol·licituds amb aquest sistema. Un cop realitzada la gestió el servei es factura i es passa a l'ERP per la seva liquidació. Com en el cas anterior es tracta d'una aplicació web, en aquest cas accessible únicament des de la xarxa interna de la organització. A través d'aquesta aplicació el departament d'operacions autoritza o denega l'entrada d'un buc a port.
- Desenvolupament sobre l'ERP Dynamics Nav. La missió principal d'aquest software és la de controlar els processos de compra i liquidació

de serveis portuaris. Aquest sistema és accessible únicament des de la xarxa interna de la organització.

- Administració electrònica: Aplicació de gestió d'expedient, registre electrònic i tramitació electrònica. Es tracta d'una aplicació web publicada a Internet.
- Control d'Accessos: Es tracta d'un sistema que gestiona el control d'accessos al recinte portuari. Tothom que accedeix al recinte portuari ha d'estar acreditat. Aquest sistema, a més, manté els perfils d'autorització, és adir, qui pot accedir a cadascuna de les instal·lacions que hi ha al recinte. No tothom pot accedir al mateix lloc. També regula, realitzant les pertinents consultes a l'agencia tributaria, la sortida de mercaderies del port (recinte duaner) cap a l'exterior. El sistema està format per diverses aplicacions:
    - Sistema per registrar transportistes i persones amb interès legítim dintre del recinte portuari. Es tracta d'una aplicació web publicada a internet.
    - LSP: Desenvolupament per consultar en la sortida del recinte si una mercaderia pot sortir. L'aplicació és accessible des de la xarxa interna i consulta un web service publicat per l'agencia tributaria a Internet.
    - Control de barreres: Sistema que interactua amb els dos anteriors per obrir les barreres del recinte.

- Sistema de telefonia: Es tracta d'un sistema de telefonia IP. Es important garantir la continuïtat d'aquest sistema, ja que, a part de donar servei a la organització, dona servei als diferents organismes que gestionen emergències dintre del recinte portuari. Aquestes últimes conversacions es graven i cal garantir la seva conservació pel correcte seguiment i auditoria d'una emergència.

Tot i que no hi ha una política formal al respecte, les aplicacions desenvolupades pel departament de sistemes d'informació, que són accessibles a través de la xarxa (tant interna com pública) utilitzen protocols de comunicació segurs (SSL, TLS...)
El departament gestiona i manté moltes més aplicacions però no donen suport directe a processos de negoci.
El departament de sistemes d'informació disposa de capacitat per a contractar a professionals en matèries d'assessorament tecnològic i seguretat. De fet, el director de sistemes d'informació rep assessorament en temes de tendències tecnològiques i de seguretat de forma regular i participa en fòrums especialitzats.
A més rep regularment informació sobre alertes de seguretat, incidents i vulnerabilitats a través d'un CERT depenent del Ministeri. Les sondes i els sistemes SIEM desplegades a la xarxa permeten d'una forma mes o menys automàtica estar al corrent de l'impacte d'aquestes amenaces en els sistemes

de l’APZ. Aquests sistemes realitzen anàlisis de vulnerabilitats periòdics i proves d’intrusió automàtiques i parametritzades.
Pel que fa a la gestió d’actius, el departament de sistemes d’informació manté un inventari actualitzat de tots els actius de sistemes d’informació tant tangibles com intangibles. Per temes comptables, aquest inventari es comparteix amb el departament de finances (només dades rellevants a efectes d’inventari d’actius i amortització dels mateixos). El departament de sistemes d’informació és el responsable d’aprovisionar el sistemes de processament d’informació necessaris al personal (ordinadors, telèfons, tauletes...), sota petició del cap del departament destinatari i amb el vist i plau del departament de recursos humans i organització.
A través del responsable de qualitat del departament de sistemes d’informació i amb la col·laboració del departament de serveis jurídics, es garanteix que tots els temes de compliance que afecten a la organització i a la informació que aquesta gestiona (privacitat, retenció de dades, protecció...) es compleixen.

3. Objectius del pla director de seguretat

Tot i que la organització ha realitzat diferents tasques relacionades amb la seguretat de la informació, com poden ser la declaració dels fitxers a l'agència nacional de protecció de dades, protecció dels llocs de treball amb antivirus, protecció perimetral i backup de la informació, no hi ha definida una estratègia ni una política en quant a seguretat de la informació ni existeix un pla coordinat que indiqui on està l'APZ i on vol estar. L'APZ es conscient que la caiguda dels servidors que donen suport als processos de negoci com PCS, INTEGRA i CONTROL d'ACCESSOS pot tenir efectes molt perjudicials no només per a l'Autoritat Portuària, sinó per a tots els usuaris i empreses del Port i fins i tot per al seu Hinterland, podent arribar fins i tot a paralitzar el port, l'entrada i sortida de camions i l'entrada i sortida de vaixells. Aquest fet pot tenir un impacte econòmic significatiu i pot enfrontar-se a les reclamacions econòmiques de les empreses transportistes i navilieres, a més de l'impacte a nivell d'imatge i mal estar que pot causar el col·lapse de la ciutat de Zapata degut a les cues de camions en les seves carreteres.
D'especial importància és el sistema de control d'accessos. La llei vigent obliga a la Autoritat Portuària de Zapata a identificar i registrar de totes les persones que accedeixen al recinte portuari. Per tant cal protegir el sistema per evitar que un atacant comprometi el sistema i pugui accedir sense interès legítim.
Un altre factor a considerar és que tot i que la informació que genera l'APZ és pública, a través del seu PCS els clients demanen serveis a l'APZ i demanen serveis a altres administracions i empreses cosa que fa que aquest sistema tingui informació comercial de les empreses que treballen amb l'APZ i entre elles. Aquesta informació cal protegir-la per evitar que un possible robatori comprometi els plans de negoci i interessos de les empreses usuàries d'aquest sistema.
L'APZ, conscient de la importància de la seguretat de la informació , vol iniciar un procés de certificació ISO 27000 i d'aquesta forma augmentar el seu valor competitiu en el sector portuari.
Es per això que es necessari definir un full de ruta fins el nivell de seguretat que la organització necessita.
Per tant, els objectius del PDS són els següents:

- Identificar el riscos als que s'exposen els sistemes d'informació de l'APZ.
- Protegir la informació allotjada en el PCS.
- Protegir el sistema de control d'accessos de possibles atacs que puguin comprometre la seva informació i funcionament.
- Definir un marc de seguretat de la informació dins de l'organització.
- Incrementar el valor competitiu aconseguint una certificació ISO 27000.
- Reduir els costos derivats d'un incident de ciberseguereta t.

4. Anàlisi de compliment inicial

Per a realitzar l'anàlisi diferencial s'ha utilitzarem el model CMM (Capability Maturity Model). La descripció d'aquest model la podem veure en la següent taula:

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem.
10%	L1	Inicial / Ad-hoc	Procediments inexistents o localitzats en àrees concretes.
50%	L2	Reproduïble però intuïtiu.	Existeix un mètode de treball poc formalitzat, basat en la experiència.
90%	L3	Procés definit	Els processos estan implantats, comunicats i documentats.
95%	L4	Gestionat i mesurable	Es pot seguir l'evolució dels processos mitjançant indicadors.
100%	L5	Optimitzat	Els processos es troben en constant millora.

Taula 4-Taula CMM

CONTROL	
[5] Política de seguretat	**10 %**
[5.1] Política de seguretat de la informació	10%
[5.1.1] Document de la política de seguretat de la informació	10 %
[5.1.2] Revisió de la política de seguretat de la informació	10 %
[6] Organització de la seguretat de la informació	**18%**
[6.1] Organització interna	37%
[6.1.1] Compromís de la direcció amb la seguretat de la informació	10%
[6.1.2] Coordinació en seguretat de la informació	0%
[6.1.3] Assignació de responsables de seguretat de la informació	0%
[6.1.4] Procés d'autorització per les instal·lacions de processament d'informació	90%
[6.1.5] Acords de confidencialitat	90%
[6.1.6] Contacte amb les autoritats	0%
[6.1.7] Contacte amb grups d'interès	90%
[6.1.8] Revisió independent de seguretat de la informació	10%
[6.2] Terceres parts	0%
[6.2.1] Identificació del risc associat a les terceres parts	0%
[6.2.2] Abordar la seguretat quan es tracta de clients	0%

[6.2.3]Abordar la seguretat en acords amb terceres parts	0%
[7] Gestió d'actius	**66%**
[7.1] Responsabilitat dels actius	63%
[7.1.1] Inventari dels actius	90%
[7.1.2] Propietat dels actius	50%
[7.1.3] Ús acceptable dels actius	50%
[7.2] Classificació de la informació	70%
[7.2.1] Directives de classificació de la informació	90%
[7.2.2] Etiquetatge de la informació i manipulació	50%
[8] Seguretat dels recursos humans	**67%**
[8.1] Abans de la contractació	76%
[8.1.1] Rols i responsabilitats	90%
[8.1.2] Screening	90%
[8.1.3] Termes i condicions de la contractació	50%
[8.2] Durant la contractació	36%
[8.2.1] Responsabilitats en la gestió	10%
[8.2.2] Conscienciació, formació i entrenament en seguretat de la Informació	10%
[8.2.3] Procés disciplinari	90%
[8.3] Finalització o canvi d'ocupació	90%
[8.3.1] Finalització de responsabilitats	90%
[8.3.2] Retorn dels actius	90%
[8.3.3] Eliminació dels drets d'accés	90%
[9] Seguretat física i ambiental	**65%**
[9.1] Zones segures	72%
[9.1.1] Perímetre de seguretat física	95%
[9.1.2] Controls d'entrada físics	95%
[9.1.3] Control d'oficines, sales i instal·lacions	90%
[9.1.4] Protecció contra amenaces externes i ambientals	50%
[9.1.5] Treballant en zones segures	50%
[9.1.6] Zones d'accés públic, lliurament i càrrega	50%
[9.2] Equipament de seguretat	58%
[9.2.1] Localització d'equips i protecció	50%
[9.2.2] Instal·lacions de suport	95%
[9.2.3] Seguretat del cablejat	50%
[9.2.4] Manteniment d'equips	95%
[9.2.5] Seguretat dels equips fora de les instal·lacions	10%
[9.2.6] Eliminació o reutilització segura	95%
[9.2.7]Eliminació de la propietat	10%
[10] Gestió de les comunicacions i operacions	**56%**
[10.1] Procediments i responsabilitats en l'operació	50%
[10.1.1] Procediments d'operació documentats	50%
[10.1.2] Gestió del canvi	90%
[10.1.3] Segregació de funcions	10%
[10.1.4] Separació de l'entorn de desenvolupament, test i producció	50%
[10.2] Gestió del servei entregat per terceres parts	63%

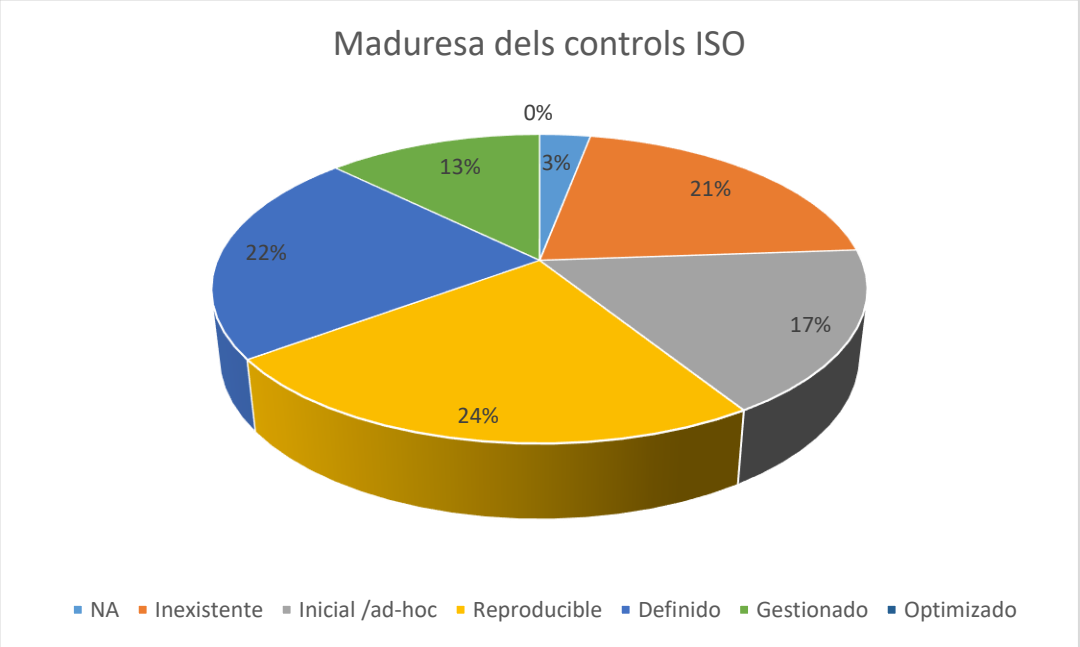
[10.2.1] Entrega del servei	10%
[10.2.2] Monitorització i revisió dels serveis entregats per terceres parts	90%
[10.2.3] Gestió dels canvis als serveis de terceres parts	90%
[10.3] Planificació i acceptació del sistema	50%
[10.3.1] Gestió de la capacitat	50%
[10.3.2] Acceptació del sistema	50%
[10.4] Protecció contra codi maliciós i mòbil	47%
[10.4.1] Protecció contra codi maliciós	95%
[10.4.2] Protecció contra codi mòbil	0%
[10.5] Backup	95%
[10.5.1] Backup de la informació	95%
[10.6] Gestió de la seguretat de la xarxa	92%
[10.6.1] Controls de xarxa	95%
[10.6.2] Seguretat dels serveis de xarxa	90%
[10.7] Manipulació de mitjans	28%
[10.7.1] Gestió de mitjans extraïbles	10%
[10.7.2] Destrucció de mitjans	10%
[10.7.3] Procediments de manipulació de la informació	0%
[10.7.4] Seguretat de la documentació del sistema	95%
[10.8] Intercanvi d'informació	32%
[10.8.1] Procediments i polítiques d'intercanvi d'informació	0%
[10.8.2] Acords d'intercanvi	10%
[10.8.3] Mitjans físics en trànsit	10%
[10.8.4] Missatgeria electrònica	90%
[10.8.5] Sistemes d'informació empresarial	50%
[10.9] Serveis de comerç electrònic	50%
[10.9.1] Comerç electrònic	NA
[10.9.2] Transaccions on-line	NA
[10.9.3] Informació pública disponible	50%
[10.10] Monitorització	58%
[10.10.1] Auditoria de registres	95%
[10.10.2] Monitorització de l'ús del sistema	95%
[10.10.3] Protecció de la informació dels registres	10%
[10.10.4] Registres d'administrador i d'operador	95%
[10.10.5] Registre de fallades	50%
[10.10.6] Sincronització de rellotges	0%
[11] Control d'accessos	**52%**
[11.1] Requeriments empresarials pel control d'accessos	50%
[11.1.1] Política de control d'accessos	50%
[11.2] Gestió d'accessos d'usuari	58%
[11.2.1] Registre d'usuari	95%
[11.2.2] Gestió de privilegis	50%
[11.2.3] Gestió dels passwords d'usuari	90%
[11.2.4] Revisió dels privilegis d'usuari	0%
[11.3] Responsabilitats d'usuari	47%

[11.3.1] Utilització de passwords	90%
[11.3.2] Equips d'usuari desatesos	0%
[11.3.3] Política de taula i pantalla neta	50%
[11.4] Control d'accés a la xarxa	66%
[11.4.1] Política sobre ús de serveis de xarxa	50%
[11.4.2] Autenticació d'usuaris per a connexions remotes	95%
[11.4.3] Identificació d'equips a la xarxa	0%
[11.4.4] Diagnosi remota i protecció del port de configuració	50%
[11.4.5] Segmentació de xarxa	90%
[11.4.6] Control de connexió a la xarxa	90%
[11.4.7] Control d'enrutament de xarxa	90%
[11.5] Control d'accés a sistemes operatius	71%
[11.5.1] Procediments de log on segur	95%
[11.5.2] Identificació i autenticació d'usuari	95%
[11.5.3] Sistema de gestió de passwords	95%
[11.5.4] Ús d'utilitats del sistema	50%
[11.5.5] Time out de sessió	90%
[11.5.6] Limitació del temps de connexió	0%
[11.6] Control d'accés a les aplicacions i a la informació	70%
[11.6.1] Restriccions d'accés a la informació	90%
[11.6.2] Aïllament de sistemes sensibles	50%
[11.7] Teletreball i mobilitat	5%
[11.7.1] Mobilitat i comunicacions	10%
[11.7.2] Teletreball	0%
[12] Adquisició de sistemes d'informació, desenvolupament i manteniment	**12%**
[12.1] Requeriments de seguretat dels sistemes d'informació	50%
[12.1.1] Anàlisi i especificació dels requeriments de seguretat	50%
[12.2] Processament correcte a les aplicacions	
[12.1.1] Validació d'entrada de dades	50%
[12.2.2] Control del processament intern	0%
[12.2.3] Integritat dels missatges	0%
[12.2.4] Validació de les dades de sortida	0%
[12.3] Controls criptogràfics	5%
[12.3.1] Polítiques en l'ús de controls criptogràfics	10%
[12.3.2] Gestió de claus	0%
[12.4] Seguretat dels sistemes de fitxers	17%
[12.4.1] Control del software operacional	50%
[12.4.2] Protecció de les dades de prova del sistema	0%
[12.4.3] Control d'accés al codi font	0%
[12.5] Seguretat en els processos de desenvolupament i de suport	42%
[12.5.1] Procediment de control de canvis	10%
[12.5.2] Revisió tècnica de les aplicacions després des canvis en el sistema operatiu	50%
[12.5.3] Restriccions en els canvis en els paquets de software	10%

[12.5.4] Fuga d'informació	50%
[12.5.5] Desenvolupament extern de software	90%
[12.6] Gestió de vulnerabilitats tècniques	10%
[12.6.1] Control de vulnerabilitats tècniques	10%
[13] Gestió d'incidents de seguretat de la informació	16%
[13.1] Report d'incidents de seguretat de la informació i feblesa	30%
[13.1.1] Report d'events de seguretat de la informació	50%
[13.1.2] Report de febleses	10%
[13.2] Gestió d'incidents de seguretat de la informació i millores	3%
[13.2.1] Responsabilitats i procediments	10%
[13.2.2] Aprenentatge de incidents de seguretat de la informació	0%
[13.2.3] Recol·lecció d'evidències	0%
[14] Gestió de la continuïtat de negoci	**0%**
[14.1] Aspectes de seguretat de la informació en la gestió de la continuïtat de negoci	0%
[14.1.1] Inclusió de la seguretat de la informació en el procés de gestió de continuïtat de negoci	0%
[14.1.2] Continuïtat de negoci i avaluació de riscos	0%
[14.1.3] Desenvolupament i implementació de plans de continuïtat de negoci incloent la seguretat de la informació	0%
[14.1.4] Marc de planificació de continuïtat de negoci	0%
[14.1.5] Proves, manteniment, re-avaluació dels plans de continuïtat de Negoci	0%
[15] Conformitat	**56%**
[15.1] Compliment amb els requeriments legals	90%
[15.1.1] Identificació de la legislació aplicable	90%
[15.1.2] Drets de propietat intel·lectual	90%
[15.1.3] Protecció del registres de la organització	90%
[15.1.4] Protecció de dades y privacitat de la informació personal	90%
[15.1.5] Prevenció del mal ús de les instal·lacions de processament d'informació	90%
[15.1.6] Regulació dels controls criptogràfics	NA
[15.2] Conformitat amb polítiques i estàndards de seguretat y conformitat tècnica	30%
[15.2.1] Conformitat amb polítiques de seguretat i estàndards	10%
[15.2.2] Revisió de la conformitat tècnica	50%
[15.3] Consideracions d'auditoria dels sistemes d'informació	50%
[15.3.1] Controls d'auditoria de sistemes d'informació	50%
[15.3.2] Protecció de les eines d'auditoria de sistemes d'informació	50%

Taula 5-anàlisi diferencial

Resultat de l'anàlisi inicial

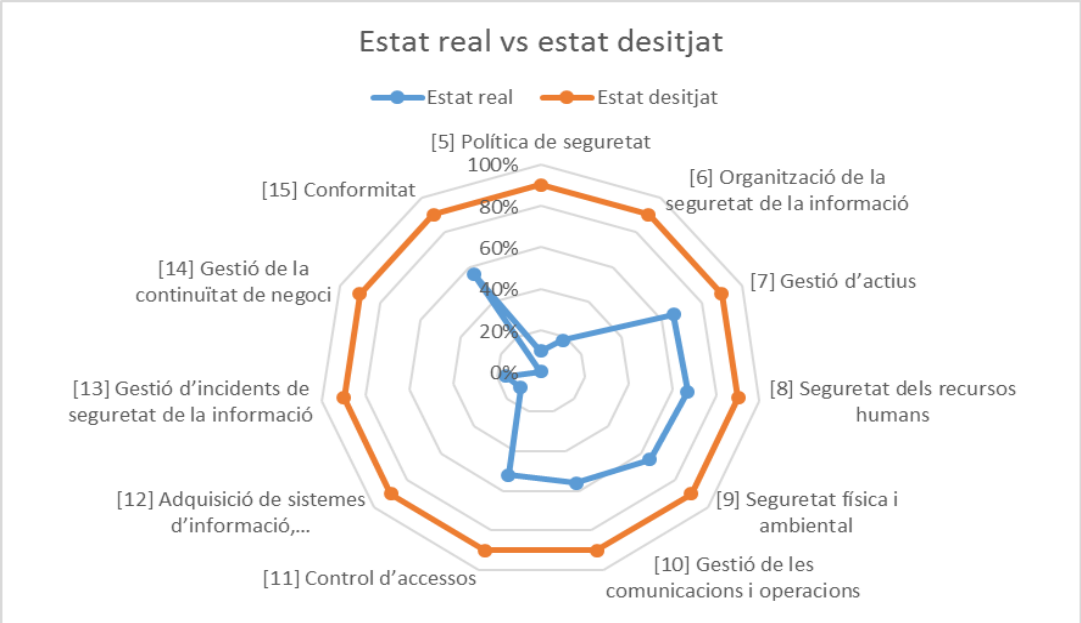


Il·lustració 13-distribució de la maduresa dels controls

Com a fet a comentar, es pot observar que la organització té un percentatge significatiu (21%) de controls que són inexistents. Tal com s'ha comentant amb anterioritat, s'ha realitzat iniciatives en seguretat de la informació, com es pot

veure en el percentatge de controls que hi ha en els nivells de maduresa L2,L3 i L4, però la gran majoria d'ells es troben en un estat no formal.

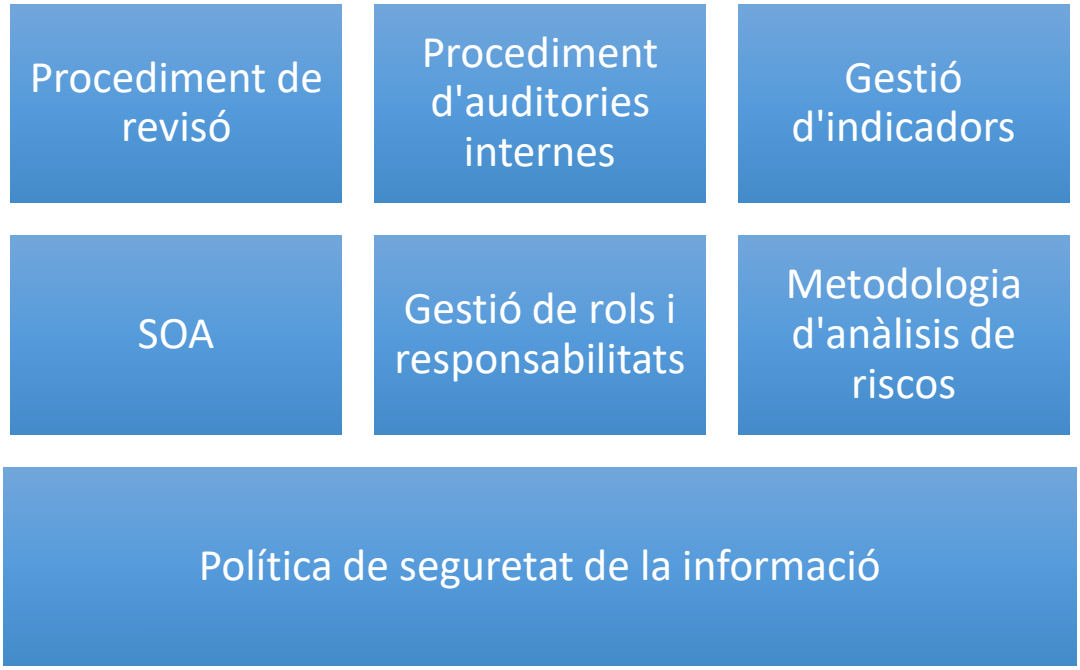
Distància entre l'estat real i l'estat desitjat



Il·lustració 14-Distància entre l'estat real i el desitjat

5. Esquema documental

Durant el desenvolupament del pla director de seguretat es desenvoluparà la documentació necessària per a donar compliment al esquema documental requerit per la norma ISO 27001.



Il·lustració 15-Cos documental del SGSI

5.1. Política de seguretat

Podem trobar la política de seguretat en l'annex política de seguretat.

5.2. Procediment d'auditories internes

Podem trobar el procediment d'auditories internes en l'annex procediment auditories internes.

5.3. Procediment de revisió

Podem trobar el procediment per a la revisió en l'annex procediment de revisió.

5.4. Gestió d'indicadors

Podem trobar la fitxa per a la gestió d'indicadors a l'annex gestió indicadors.

5.5. Declaració d'aplicabilitat

Podem trobar la declaració d'aplicabilitat a l'annex declaració aplicabilitat SOA.

5.6. Metodologia d'anàlisi de riscos

Podem trobar la metodologia d'anàlisi de riscos a l'annex metodologia d'anàlisi de riscos.

5.7. Gestió de rols i responsabilitats

Podem trobar la gestió de rols i responsabilitats al l'annex procediment de rols i responsabilitats.

6. Anàlisi de riscos

No podem protegir allò que no coneixem. Es per això, que la primera etapa cap al Pla d'Implementació de un SGSI consisteix en la avaluació dels nostres actius, considerant les dependències existents entre ells i fent la valoració dels mateixos.

6.1. Inventari d'actius

El procediment d'anàlisi i gestió de riscos d'aquest PDSI es desenvoluparà basant-se en la metodologia MAGERIT V3. Això té conseqüències en la forma de classificar i valorar els actius i en la nomenclatura que assignem. Prenent com a base els actius proposats en l'enunciat del treball:

Tipus d'actiu	Classificació MAGERIT v3
Instal·lacions	[L]
Hardware	[HW]
Aplicació	[SW]
Dades	[D]
Xarxa	[COM]
Serveis	[S]
Equipament auxiliar	[AUX]
Personal	[P]

Taula 6-tipus d'actius segons MAGERIT

Taula de valoració dels actius en funció del servei que presten: En aquesta taula no es té tant en compte el valor econòmic de l'actiu, però si el valor que té en conjunt per al negoci.

Valor	Classificació
Molt Alt	MA
Alt	A

Mig	M
Baix	B
Molt Baix	MB

Taula 7-valor dels actius segons MAGERIT

Els actius és calibraran segons les diferents dimensions de seguretat:

Dimensió	Classificació	Descripció
Confidencialitat	C	La informació ha d'estar disponible únicament per a aquelles persones autoritzades.
Integritat	I	Cal garantir que la informació no ha estat manipulada de forma no legítima.
Disponibilitat	D	La informació ha d'estar disponible quan es necessita.
Autenticitat	A	La persona/organització és realment qui diu ser.
Traçabilitat	T	Les actuacions d'una persona/organització poden ser imputades a aquella persona/organització.

Taula 8-dimensions de la seguretat

A partir d'aquesta taula, es pot calcular l'impacte de la pèrdua de l'actiu per a la organització. Per a dur-ho a terme, ens basarem en el criteri de valoració proposat per MAGERIT v3:

Valor		Criteri
10	Extrem	Dany extremadament greu.
9	Molt alt	Dany molt greu.
6-8	Alt	Dany greu.
3-5	Mig	Dany important.
1-2	Baix	Dany menor.
0	Irrellevant	Irrellevant a efectes pràctics.

Taula 9-definició del valor de l'impacte

La taula amb els valors resultants es pot consultar a l'annex valoració d'actius.

6.2. Anàlisi d'amenaces

En aquest apartat es mostra un anàlisi de les amenaces que poden afectar els actius de l'organització. Per a dur a terme aquest anàlisi es prendrà com a punt de partida la taula d'amenaces que especifica MAGERIT v3. Aquesta taula es pot trobar al llibre II "Catálogo de Elementos", punt 5.

Per a realitzar la valoració es fa servir la següent taula de freqüència d'amenaces, que pot considerar-se adequada per a una organització com l'APZ:

Freqüència	ID	Valor	Descripció
Extrema	FE	100	diària
Alta	FA	10	mensual
Mitjana	FM	1	trimestral
Baixa	FB	1/10	semestral
Molt baixa	FMB	1/100	anual

Taula 10-definició de freqüències

Per obtenir una representació més còmoda dels actius i les amenaces que els hi afecten s'ha fet la següent distinció d'actius:

- L datacenter: instal·lació datacenter.
- L sala tècnica: instal·lació sala tècnica.
- L oficines: instal·lació d'oficines.
- HW servidors: Servidors allotjats al datacenter.
- HW sala tècnica: Hardware allotjat a les sales tècniques.
- HW usuari: PC usuari.
- COM: comunicacions.
- SW servidor: Software instal·lat en els servidors allotjats al dataceter.
- SW usuari: Software instal·lat als ordinadors del usuaris.
- P: personal.
- D: dades.
- AUX: Instal·lacions auxiliars.

Amb la taula de MAGERIT v3 i la taula de freqüències anterior obtenim la valoració d'amenaces (impacte x dimensió):, que podem consultar a l'annex valoració d'amenaces. S'han organitzat els actius per grup d'actius subjectes a un conjunt d'amenaces concret. El grup d'amenaces que afecta cada tipus d'actiu s'ha obtingut de MAGERIT v3.

6.3. Impacte potencial

En aquest punt estem en condicions de calcular l'impacte potencial. Coneixent el valor dels actius i la degradació que causa les possibles amenaces es pot calcular l'impacte que pot causar a l'organització la materialització de l'amenaça sobre l'actiu.

Per a realitzar el càlcul de l'impacte sobre cadascun dels actius s'ha utilitzat la següent fórmula:

$$IMPACTE\ POTENCIAL = VALOR\ DE\ L'ACTIVU * IMPACTE\ SOBRE\ L'ACTIU$$

On el valor de l'actiu l'obtenim de la taula calculada a l'apartat Inventari d'actius, d'aquesta forma podem calcular l'impacte potencial per a cadascuna de les dimensions de seguretat de l'actiu.
La taula resultant la podem consultar a l'annex impacte potencial.

6.4. Nivell de risc acceptable i residual

Una vegada calculat l'impacte potencial, es procedeix a determinar el risc associat a la materialització d'una amenaça. Un cop fet aquest càlcul, cal determinar el risc acceptable i per tant veure en risc residual. Tenint en compte els objectius de seguretat de la organització caldrà prioritzar les tasques a realitzar en funció d'aquests objectius (recordem que era molt important garantir la continuïtat del control d'accessos i de les eines de sol·licitud de serveis).
El risc es calcula amb la següent fórmula:

$$RISC = FREQÜÈNCIA * IMPACTE$$

D'aquesta formula s'obté el risc residual associat a cada element de l'inventari.
La taula resultant de la formula es pot consultar a l'annex risc residual.

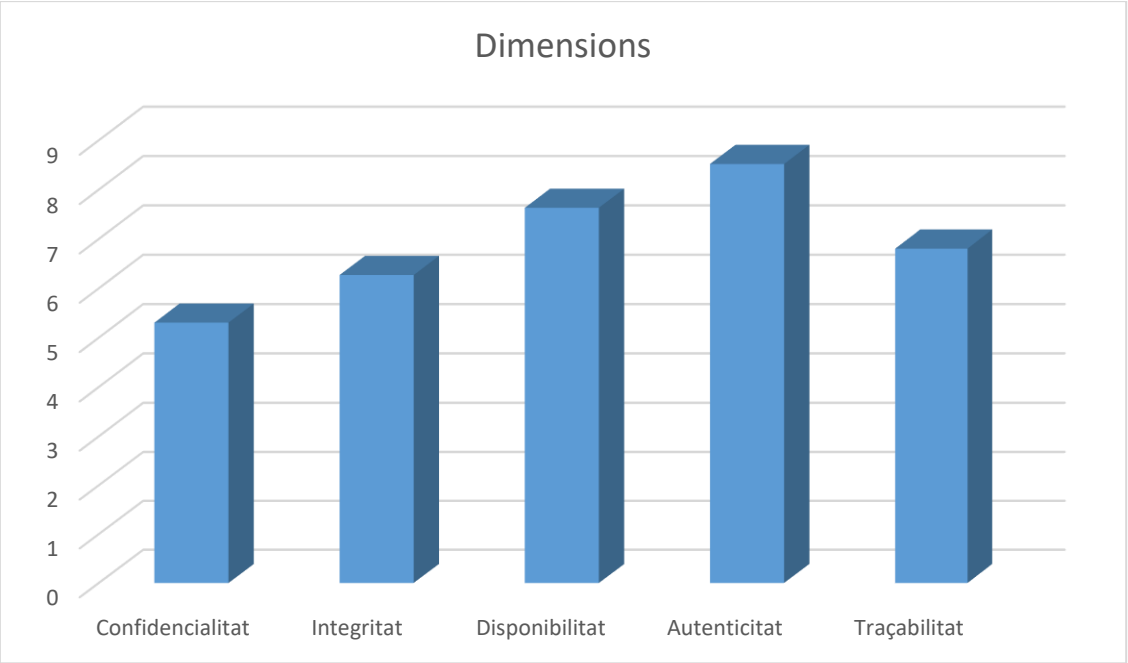
La Organització, de forma tradicional ha mantingut, pel que fa a la seguretat física, un perfil de risc conservador. Els nous acords de comerç amb països com els EEUU que requereixen alts nivells de seguretat i el fort impacte que suposa parar sistemes com el del control d'accessos i sol·licitud d'entrada de bucs fan que la Organització mantingui un perfil conservador igualment per a la seguretat lògica, pel que fixa el llindar de risc acceptable en 39 (inclòs).
Tenint en compte la taula anteriorment comentada, caldrà gestionar els següents riscos:

ID	VALOR	F	IMPACTE POTENCIAL					RISC				
			C	I	D	A	T	C	I	D	A	T
L5	A	FA	0,2	9	7	0	0	2	90	70	0	0
L7	A	FA	1	1,6	10	0	0	10	16	100	0	0
SW1	MA	FA	1,8	4,5	10	9	0	18	45	10	90	0
SW2	B	FA	1	2,5	7	5	0	10	25	70	50	10
SW3	MA	FA	1,8	4,5	10	9	0	18	45	100	90	18
SW4	M	FA	1,6	4,5	6	10	0	16	45	60	100	16
SW5	MA	FA	1	4,5	10	9	0	10	45	100	90	10
SW6	B	FA	2	5	7	10	0	20	50	70	100	20
SW7	MA	FA	2	4	10	10	0	20	40	100	100	20
SW8	MA	FA	1	3,5	10	9	0	10	35	100	90	10
SW9	A	FA	1	4,5	7	9	0	10	45	70	90	10
SW10	MA	FA	1	4,5	10	9	0	10	45	100	90	10
SW11	MA	FA	1	4,5	7	9	0	10	45	70	90	10
SW12	B	FA	1	3,5	7	5	0	10	35	70	50	10
SW13	A	FA	1	3,5	10	7	0	10	35	100	70	10
SW14	A	FA	1	3,5	10	10	0	10	35	100	100	10

Taula 11-riscos que cal gestionar

6.5. Resultats

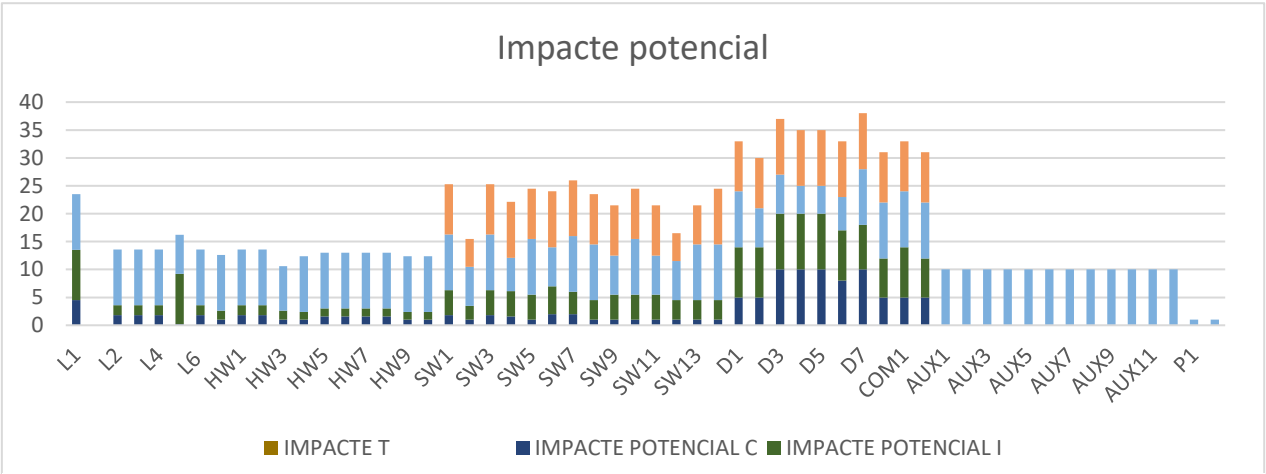
Valor mig dels actius segons la seva dimensió de seguretat



Il·lustració 16-valor mig dels actius segons dimensió

Es pot observar que el que més preocupa a l'APZ és l'autenticitat de les dades i la disponibilitat dels seus sistemes. Això es tradueix en que és molt rellevant identificar correctament els actors sobre un sistema i garantir que són qui diuen ser i vetllar per que els sistemes estiguin disponibles en el moment que són necessaris.

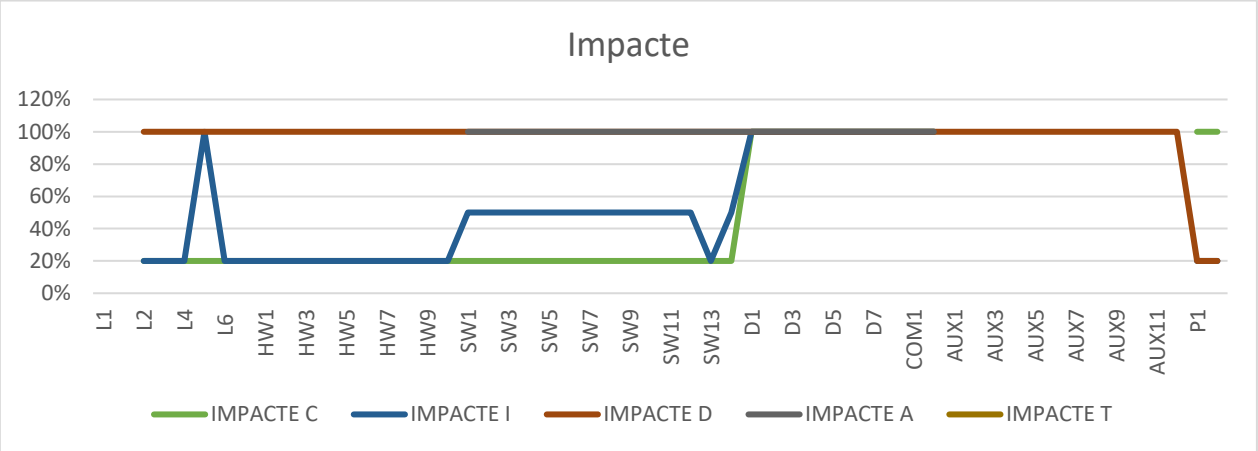
Impacte potencial



Il·lustració 17-impacte potencial

En la gràfica anterior es pot veure, per a cada actiu, quines dimensions es veuen afectades en la materialització d'una amenaça i es pot tenir una idea de la seva magnitud.

Impacte per dimensió

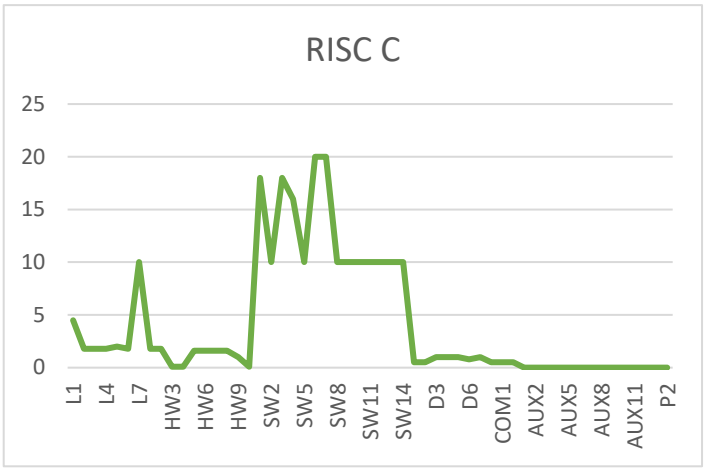


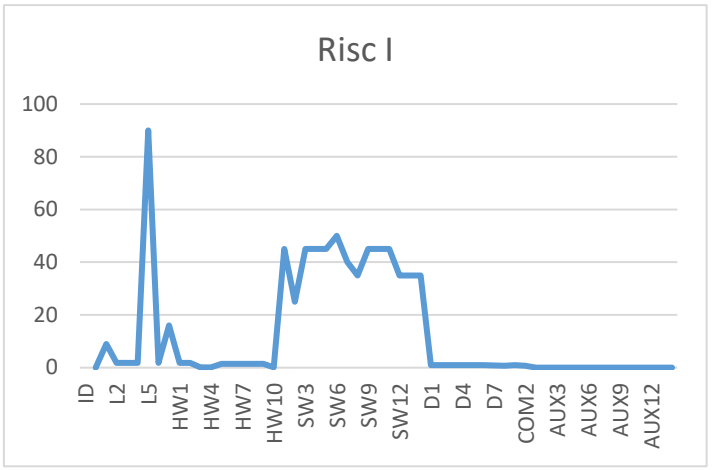
Il·lustració 18-impacte per dimensió

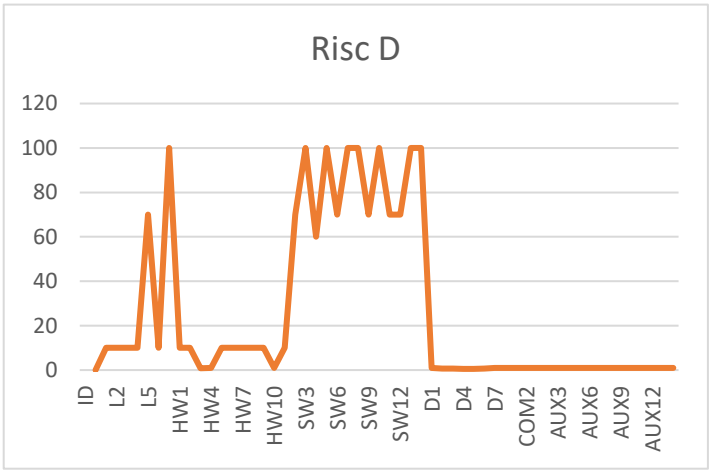
les diferents amenaces per a cadascuna de les dimensions.

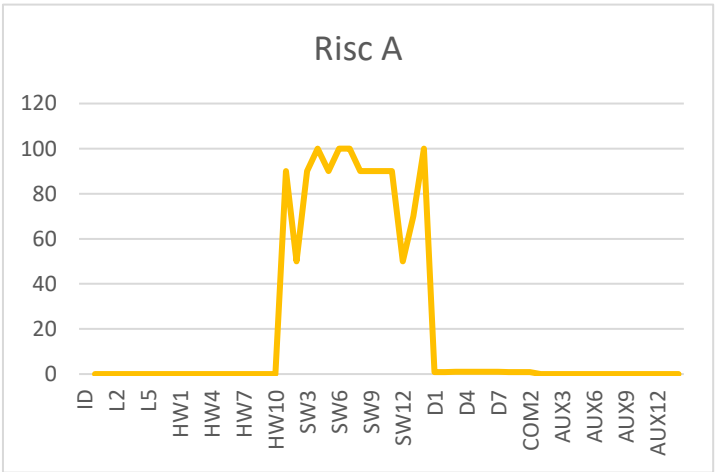
Pot observar-se que la disponibilitat es veu afectada en gairebé la totalitat dels actius.

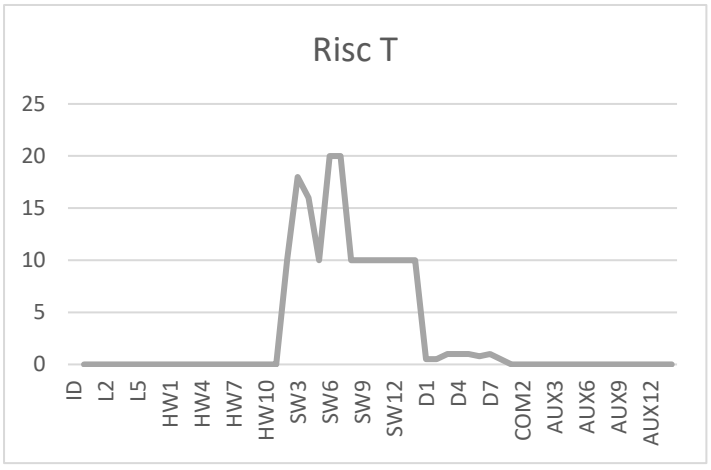
Risc segons dimensió











Il·lustració 19-risc segons dimensió

Recordem que tot valor que estigui per sobre de 39 no és assumible. En general, estan per sobre aquest llindar els actius de tipus software i dades pel que fa a la disponibilitat i autenticitat.

7. Propostes de millora

En el punt anterior s'ha mostrat el llistat d'actius crítics per a la organització i el risc residual calculat a partir d'un anàlisi de riscos. Ara és el moment de proposar millores per tal de mitigar el risc d'aquells actius que estan per sobre del risc assumible per la organització. Cal realitzar una planificació financera i temporal de les propostes i prioritzar aquelles que puguin suposar quick wins per a la organització, essent conscients que no es podran abordar tots els riscos en una primera fase i que caldrà centrar-se en aquells que essent relativament de fàcil resolució poden aportar una ràpida millora.
El conjunt de propostes es pot consultar en l'annex propostes de millora.

7.1. Planificació temporal

S'ha prioritzat aquells projectes que són dependències per a uns altres i que es consideren bàsics per afrontar la creació d'un marc de seguretat de la informació. D'entre les moltes iniciatives que caldria implementar per garantir un compliment amb la norma ISO 2002 i un procés de millora contínua s'han prioritzat aquelles que tenen relació amb la creació d'estructura de seguretat i conscienciació. D'entre els projectes tecnològics es prioritzaran en una primera fase els que impacten sobre la disponibilitat i l'autenticitat que com s'ha vist a l'AR són les dimensions de la seguretat que més preocupen a la organització.

ID PROYECTO	DURACIÓN	2017												2018											
SI-PM-01	12 mesos																								
SI-PM-02	2 mesos																								
SI-PM-03	3 mesos																								
SI-PM-04	3 mesos																								
SI-PM-05	6 mesos																								
SI-PM-06	1 mes																								
SI-PM-07	2 mesos																								
SI-PM-08	24 mesos																								
SI-PM-09	1 mes																								
SI-PM-10	24 mesos																								

Taula 12-planificació temporal de les propostes de millora

Els projectes de caràcter tecnològic s'han planificat per al període estival, ja que es quan hi ha un major nombre de treballadors de vacances. D'aquesta forma l'impacte en l'Organització, en cas de problemes, és menor. A més, durant aquest període el departament té menys càrrega de treball relacionat amb l'atenció a l'usuari i projectes de desenvolupament, per tant pot centrar els esforços en projectes interns.

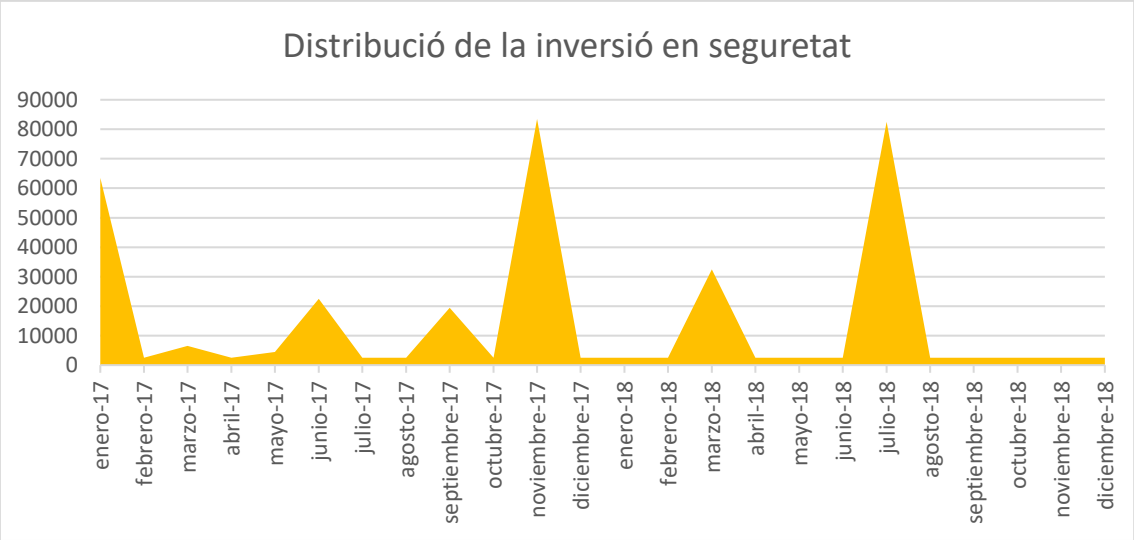
La Organització és conscient de que cal plantejar projectes per millorar en altres àrees, però s'ha centrat en realitzar una millora important amb un esforç assumible tant en recursos humans com econòmics, deixant per a un futur les àrees que considera poden requerir projectes més complexos.

7.2. Planificació financera

ID PROYECTO	Pressupost	Distribució
SI-PM-01	10.000€	Pagament de la part proporcional després de cada sessió.
SI-PM-02	-	
SI-PM-03	-	
SI-PM-04	30.000€	Pagament al finalitzar el projecte.
SI-PM-05	100.00€	Pagament del 20 % a l'inici del projecte i pagament de 80 % al final.
SI-PM-06	60.000€	Pagament al final del projecte.
SI-PM-07	15.000€	Pagament al final del projecte.
SI-PM-08	30.000€	Pagament de la part proporcional cada mes.
SI-PM-09	80.000€	Pagament al final del projecte.
SI-PM-10	30.000€	Pagament de la part proporcional cada mes.

Taula 13-planificació financera de les propostes de millora

TOTAL: 355.000€



Il·lustració 20-distribució de la inversió en seguretat

7.3. Evolució del risc

- Els plans de conscienciació i formació han de servir per reduir el risc associat als mals usos dels sistemes d'informació i així reduir el risc de que es materialitzi una incidència de seguretat.
- Els plans de conscienciació i capacitació al personal tècnic ha de servir per reduir el risc associat a vulnerabilitats del sistema, actualitzacions, manipulació i configuració de software.
- La resta de mesures estan pensades per crear organització de seguretat i per millorar la resposta a incidents de seguretat.

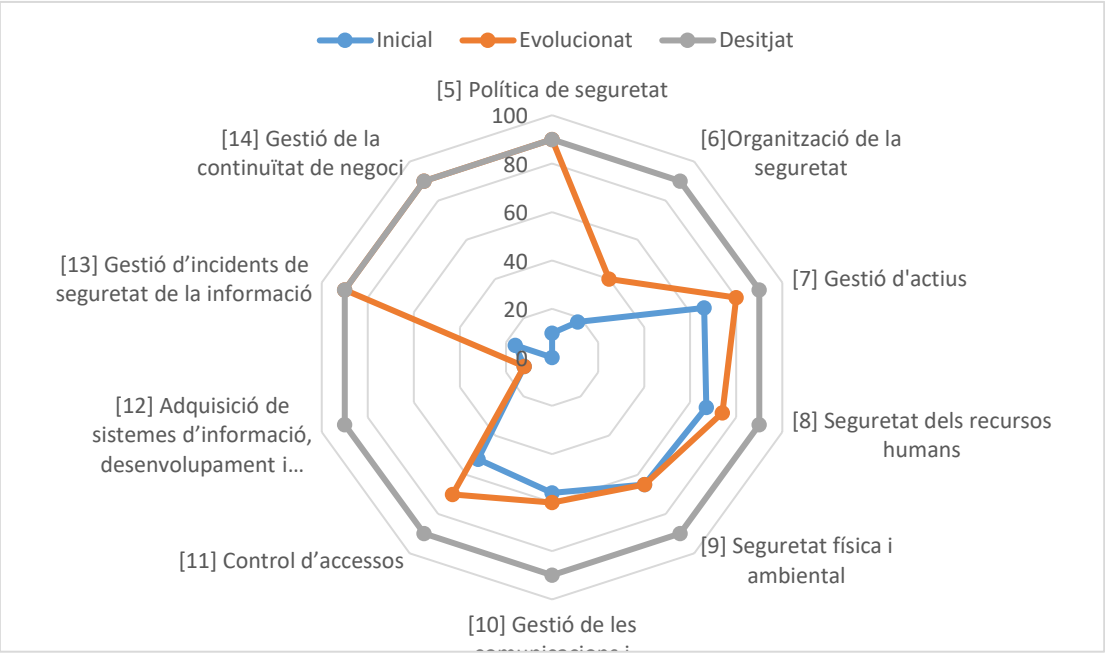
Es pot consultar l'evolució del risc, especialment en aquells casos on el risc residual no és acceptable, en l'annex evolució del risc.
Amb la implementació de les mesures proposades no hi ha cap risc residual per sobre de l'assumible per la Organització.

7.4. Nivell d'acompliment de la norma ISO 27002

DOMINI	PROJECTE	CONTROL
8-Seguretat dels recursos humans	SI-PM-01,SI-PM-10	8.2.2, 8.2.1
6-Organització de la seguretat de la informació	SI-PM-02	6.1
7-Gestió d'actius	SI-PM-03	7.1,7.2
14-Gestió de la continuïtat de negoci	SI-PM-04	14.1
11-Control d'accessos	SI-PM-05, SI-PM-02	11.1,11.3,11.7
9-Seguretat física i ambiental	SI-PM-06,SI-PM-08	9.2.2
10-Gestió de les comunicacions i operacions	SI-PM-07, SI-PM-09	10.10, 10.5
15- Conformitat	SI-PM-02	

Taula 14-relació entre millores i dominis

A continuació es pot observar una gràfica comparant la situació inicial de compliment de cadascun dels dominis, l'evolució i la situació desitjada.



Il·lustració 21-comparació entre estat inicial i post millores

Pot observar-se com amb uns esforços relativament moderats però adequats per a una organització que s'inicia en la millora de la seguretat s'aconsegueix una aproximació als seus objectius.
També pot observar-se que hi ha projectes que no aporten un gran impacte en el domini pertanyent però que a nivell pràctic interessa a l'organització implantar, com són el projecte de millora del suport elèctric o HA en la virtualització. Amb aquests projectes no s'assoleix un nivell de maduresa adequat per assolir una certificació però si que es redueix el risc en la materialització d'una amenaça.

8. Auditoria d'acompliment

Durant aquesta fase es realitzarà una auditoria d'acompliment per tal d'avaluar el grau de maduresa de la seguretat de la informació. Cal tenir en compte que aquesta avaluació es realitza un cop ha finalitzat el Pla Director de Seguretat de la Informació i s'han executat les propostes de millora de l'apartat anterior. Per a realitzar aquesta tasca es pren com a referencia la norma ISO 27002:2013, on s'especifiquen 14 dominis i 114 controls. El procés d'auditoria interna i els seus objectius es troben especificats en l'apartat 9.2 de la norma ISO 27001:2013.

Com a resultat d'aquesta fase s'obtindrà un pla d'auditoria i un informe de no conformitats.

El document d'auditoria de compliment complert es pot consultar al document adjunt APZ-2000 Auditoria interna d'acompliment.

8.1. Resum executiu

Partint de la situació inicial, on trobem una organització on a nivell general en la organització no hi ha consciència de seguretat de la informació i on el departament de sistemes d'informació implementa un conjunt de bones pràctiques per assolir "uns mínims", pot observar-se que hi ha una evolució positiva si es compara la situació inicial amb la actual. Des dels inicis del pla director de seguretat de la informació fins a la presentació d'aquests resultat, s'ha evolucionat en tots els dominis, a excepció del a.12, especialment, molt favorable ha estat l'evolució en els dominis A.5, A.6, A.7, A.13, A.14. Tot i aquest evolució l'organització ha de millorar sensiblement per poder afrontar-se amb garanties a una certificació ISO 27001.

Total de no conformitats NC

MENORS	MAJORS
7	4

Taula 15-resum no conformitats

9. Conclusions

La organització objecte d'aquest TFM ha donar les primeres passes en implantar un procés de seguretat de la informació de forma transversal a tota la organització. S'ha iniciat els passos adients per conscienciar a la direcció de la organització en termes de seguretat de la informació i prova d'això és que s´ha obtingut pressupost propi per a implantar projectes derivats de l'anàlisi de risc de la fase 3. Amb relativament petites iniciatives, sobretot en el que fa a establiment de polítiques i formalització de procediments s'ha observat una millora significativa en la seguretat de la informació de la organització. Però també s'observa que amb iniciatives aïllades no n'hi ha prou per assolir una certificació ISO/IEC 27001, encara queda millorar en certs dominis per poder afrontar amb garanties una auditoria de certificació. Un cop abordats els projectes més prioritaris i que permeten aportar valor en seguretat reduint riscos i creant consciència i imatge, cal plantejar l'elaboració d'un mapa de ruta per resoldre les no conformitats de l'auditoria interna i plantejar-se afrontar una auditoria de certificació. Aquest fet milloraria encara més la imatge de la organització vers els seus grups d'interès.

Una bona meta aconseguida ha estat que amb la implantació del SGSI, s'ha aconseguit identificar els actius crítics de la organització i assignar-hi responsables. Aquesta informació és necessària per saber el valor de l'actiu i l'impacte en cas de pèrdua. L'anàlisi de riscos ha aportat informació sobre els principals riscos des actius d'informació de l'APZ i de les dimensions que més impacten en la seguretat de la informació.

10. Annexos

10.1. Annex política de seguretat de la informació

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1104 Política de seguretat de la informació

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	18-10-2016	
1.1	02-11-2016	Inclusió del control de versions

Objectius

L'objectiu bàsic de la política de seguretat de la informació és establir els principis generals per a la protecció de la informació i els recursos associats a les tecnologies de la informació utilitzada per l'Autoritat Portuària de Zapata, en particular la intenció:

- Definir la política a seguir en relació amb la seguretat de la informació.
- Donar directrius per aconseguir nivells de seguretat adequats que permetin una bona gestió dels riscos identificats.
- Protegir els actius d'informació d'acord el seu nivell de risc.
- Preservar la privacitat dels clients, empleats, proveïdors i tercers.
- Vetllar pel compliment de les exigències en matèria legal de APZ.
- Compromís de millora continua amb la gestió del sistema de seguretat de la informació.

Àmbit d'aplicació

L'APZ i terceres organitzacions relacionades amb ella que tracten dades o informacions pertanyents o relacionades amb les seves operacions, estan subjectes a l'aplicació d'aquesta política. Abarca informació de tota l'APZ, en qualsevol dels seus formats i qualsevol suport possible, recollint activitats i relacions amb els clients, empleats, proveïdors i qualsevol tercer implicat.
Per la naturalesa i objecte de l'activitat de l'APZ, s'ha d'observar el compliment de les normes i dels estàndards de rang superior (lleis, normes i disposicions legals) que tindran preferència sobre les directrius d'aquesta política de seguretat de la informació:

1. Normativa espanyola que regula la seva activitat.
2. Normes espanyoles que provinguin d'organismes supranacionals del que Espanya sigui membre.

Any	Legislació	Document font
1981	Conveni 108/1981 del Consell d'Europa, par la protecció de las persones en relació al tractament automatitzat de dades de caràcter personal.	Conveni 108-1981
1995	Directiva 95/46/CE, del Parlament Europeu y del Consell, de 24 de octubre de 1995 relativa a la protecció de las persones físiques pel que fa referència al tractament	https://www.sede.fnmt.gob.es/sede/normas/Directiva-95-46-CE.pdf

	de les dades personals i a la lliure circulació d'aquestes dades.	
1996	Reial Decret Legislatiu 1/1996, de 12 de abril, por el que s'aprova el text refós de la Llei de Propietat Intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria.	http://www.boe.es/boe/dias/1996/04/22/pdfs/A14369-14396.pdf
1999	Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.	https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf
2002	Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic.	http://www.mityc.es/dgdsi/lssi/normativa/DocNormativa/Ley%2034_02consolidado_marzo2011.pdf
2003	Llei 59/2003, de 19 de desembre, de Signatura Electrónica.	http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf
2006	Llei 23/2006, de 7 de juliol, por la que es modifica el text refós de la Llei de Propietat Intel·lectual, aprovat pel Reial Decret Legislatiu 1/1996 de 12 d'abril.	http://www.boe.es/boe/dias/2006/07/08/pdfs/A25561-25572.pdf
2006	INSTRUCCIÓ 1/2006, de 8 de novembre, de la Agencia Espanyola de Protecció de Dades, sobre el tractament de dades personals amb finalitats d3 vigilància a través de sistemes de càmeres o videocàmeres.	https://www.agpd.es/portalwebAGPD/canalresponsable/videovigilancia/common/Instruccion_1_2006_videovigilancia.pdf
2007	Reial Decret 1720/2007, de 21 de desembre, por el que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.	http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf
2010	Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de la Administració Electrònica.	http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf
2010	Llei Orgànica 5/2010, de 22 de juny, pel qual es modifica la Llei Orgànica 10/1995, de 23 de novembre, del Codi Penal donat que modifica la tipificació dels denominats delictes informàtics.	http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf
2011	Llei 2/2011, de 4 de març, d'Economia Sostenible. Modificació de la LOPD. Disposició final.	http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Ley_eco_sostenible_extracto_BOE.pdf
2012	Resolució de 29 de novembre de 2012, de la Secretaria d'Estado de Administracions Públiques, por la que es publica l'Acord de aprovació de la Política de Signatura Electrónica i de Certificats de l'Administració General de l'Estado i s'anuncia la seva publicació a la seu corresponent.	http://www.boe.es/boe/dias/2012/12/13/pdfs/BOE-A-2012-15066.pdf

Taula 16-legislació aplicable per a la política de seguretat

Aquesta política dona cobertura a totes les activitats de l'APZ respecte al tractament de la informació i dels sistemes que li donen recolzament.
L'APZ, proveïdors i tercers relacionats han d'acomplir , com indica la present política, amb tot el que està relacionat amb el tractament de la informació propietat d'APZ (creació, procés, comunicació, distribució, emmagatzematge i desplegament).

Motivació

La importància de la seguretat de la informació creix a l'APZ degut als següents motius:

- L'APZ afronta la ràpida expansió, utilització i dependència de les TIC, pel que és necessari i raonable aconseguir que tots els empleats coneguin els mètodes apropiats de gestió, tractament i salvaguarda de la informació, així com dels recursos informàtics associats a aquests.
- Les obligacions derivades del desenvolupament legislatiu associat a la societat de la informació.
- La necessitat de protegir i evitar la difusió de la informació confidencial de l'APZ respecte a tercers que implica la implementació de controls de seguretat raonables i eficients.

Política general

La política de la APZ considera la informació com un actiu que deu ser apropiadament avaluat i protegit contra qualsevol forma no autoritzada d'accés, ús, revelació, modificació, destrucció i denegació.
Els controls de seguretat de la informació deuen ser suficientment efectius per assegurar:

- La **confidencialitat**: la informació no estarà disponible o no serà revelada a individus o entitats no autoritzades.
- La **integritat**: la informació només serà modificada pels usuaris autoritzats per a aquesta funció.
- La **disponibilitat**: la informació i els recursos de processament d'aquesta podran ser accedit pels usuaris autoritzats quan ho necessitin.

Els projectes de TI han de procedir, en coordinació amb la Direcció de Seguretat Industrial, i d'acord a la política de seguretat de classificació i intercanvi de la informació, a la gestió, classificació, sempre que estigui sota el seu control, i la identificació dels nivells adequats de protecció.

El responsable de seguretat de la informació depositari de la informació haurà d'assegurar-se, i així reportar-ho, de la implementació d'aquells controls que hagin estat identificats i considerats necessaris en relació a l'actiu d'informació i al seu tractament.

Els propietaris de la informació són responsables de la comunicació de qualsevol canvi real en els nivells requerits de protecció i mesures de seguretat relacionades amb els actius, essent necessari que els sistemes d'informació garanteixin la habilitació de les noves mesures de seguretat. Aquests controls de seguretat han d'aplicar-se tenint en compte el valor de la informació i per tant el seu nivell de classificació i els processos associats al seu tractament.

La informació considerada confidencial pel APZ requereix controls més estrictes en el seu tractament.

El Responsable de Seguretat de la Informació té el deure d'assegurar la implementació, supervisió i manteniment de les polítiques de seguretat de la informació de l'APZ, així com oferir assistència en:

- Establiment de polítiques i procediments.
- Implementació tècnica i de procediments.
- Auditoria i revisió.

Compliment

Els empleats de l'APZ han de conèixer les seves funcions i obligacions en relació a les polítiques de seguretat de la informació, fet pel que aquestes li han de ser comunicades en base a les funcions que desenvolupa.
Tots els empleats de l'APZ han de conèixer i actuar, per tant, conforme a aquesta política i als seus desenvolupaments normatius.
En cas d'actuacions contraries al contingut d'aquesta política o de qualsevol desenvolupament normatiu en seguretat de l'APZ, podran activar-se mecanismes correctius o sancionadors.

Excepcions a la política

Les excepcions a la política han de limitar-se a aquells casos en els que sigui estrictament imprescindible amb autorització expressa de la Direcció de Seguretat Industrial.
Només es permetran excepcions a la política de seguretat de la informació si es demostra que no exposen a l'APZ a nivells de risc no assumibles.

Comunicació d'incidents

Tots els casos reals o sospitosos de robatori o abús d'actius d'informació, així com possibles amenaces (hackers, virus, foc, ...) o punts febles que afectin a la seguretat hauran de ser reportats immediatament mitjançant el

procediment de comunicació d'incidents i, si es considera necessari al Director de Seguretat de la Informació i/o al Director de cada àrea funcional.

Definicions de la gestió de seguretat de la informació

En el punt Glossari d'aquest annex es presenta una sèrie de definicions que s'utilitzaran en la política i el cos normatiu.

Propietari dels actius de la informació

Cada actiu o conjunt d'actius de la informació ha de tenir assignat un responsable de l'APZ representatiu, que sigui el seu propietari i tingui la responsabilitat de realitzar i comunicar avaluacions sobre la seva identificació, valoració, utilització i protecció.
Els actius d'informació, a més de en sistemes informàtics, poden trobar-se en qualsevol altre suport com: paper, fitxers multimèdia, software...
Les polítiques de seguretat de la informació tindran aplicació sobre els actius d'informació en qualsevol suport.

Classificació de la informació

La identificació dels actius d'informació és un del principals processos a considerar pel govern d'una organització, per tant resulta fonamental la correcta identificació dels actius ja que representen la base d'informació pels anàlisis de riscos i per l'aplicació dels controls de seguretat.

a) Tipus d'informació

La informació es pot presentar de diverses formes i en diferents suports. Qualsevol que sigui la forma de presentació de la informació requereix el mateix grau de protecció, tant si es tracta de mitjans electrònics com suports de dades o paper.

- Un exemple d'informació electrònica són les dades creades des d'un sistema i trameses per correu electrònic.
- Els suports de dades poden ser magnètics, òptics, electrònics. Per exemple disquets, CD-ROM cintes magnètiques...
- Com exemple d'informació en paper podem agafar articles, faxos, dibuixos, plànols...

b) Propietat de la informació

Tota la informació generada a l'APZ és propietat de l'APZ, independentment de la seva data de creació o suport. Cada departament és responsable de la informació creada o sota la seva gestió. La classificació de tota la informació i posteriors modificacions seran fixades pels responsables dels departament que la generen i l'aproven, seguint els requeriments establerts per aquest document.
No obstant, si qualsevol persona de l'APZ considera que una determinada informació hauria d'estar classificada o la seva classificació no és l'adequada haurà de comunicar-ho al propietari.

c) Dades de caràcter personal

Les dades considerades personals, i d'acords amb les definicions legals vigents a Espanya, han de ser identificades i protegides de forma especial. Els requeriments de seguretat per aquest tipus de dades estan regulats per la llei Orgànica 15/1999 de protecció de dades de caràcter personal (LOPD) i el seu reglament de desenvolupament, Reial Decret 1720/2007 (RLOPD).

d) Classificació de la informació

La informació a l'APZ té quatre nivells de classificació:
- PÚBLICA
- INTERNA
- CONFIDENCIAL
- RESERVADA

La classificació de la informació no és estàtica i pot canviar.

- **Informació PÚBLICA**

S'aplica a la informació que una vegada publicada es lliure i la seva utilització no pot ocasionar perjudicis de cap tipus a l'APZ. Exemples d'aquest tipus d'informació són: materials de comunicació al públic en general, informació sobre els serveis que APZ ofereix als seus clients accessible a la web.

- **Informació INTERNA**

S'aplica a la informació l'ús de la qual està limitat als empleats de la APZ i al personal que exerceix tasques de subcontractació o externalització. Aquest tipus d'informació no està dirigit a personal sense relació directa amb l'APZ. Exemples d'aquest tipus d'informació són: procediments i operacions de treball, manuals de capacitació interna, directrius...

- **Informació CONFIDENCIAL**

S'aplica a la informació l'ús de la qual està limitada a un grup reduït. Generalment es tracta d'informació important per a la operativa, seguretat, tecnològica i financera de la organització. Exemples d'aquest tipus d'informació són: normes i procediments específics (exemple configuració de regles al Firewall), informació sobre nous serveis i la seva data de comercialització (abans d'emissió oficial), patents, esborranys de contractes i contractes en vigor, canvis en l'organigrama abans de la seva publicació, informes d'auditoria...

- **Informació RESERVADA**

S'aplica a la informació que en cas de publicar-se indegudament pot ocasionar un impacte negatiu greu pels objectius de l'APZ, conseqüències legals, afectar al seu patrimoni, imatge... Generalment es tracta d'informació de màxima transcendència pel desenvolupament i continuïtat de l'Organització. Aquesta informació està limitada a grups molt reduïts i localitzat de persones de Presidència i/o Direcció d'APZ. Exemples d'aquest tipus d'informació son: estratègies de l'organització, informació sobre projectes d'innovació...
L'accés a aquest tipus d'informació requereix la identificació de l'individu que hi accedeix.

e) Etiquetatge de la informació

La classificació de la informació s'identifica a través del seu etiquetatge. Per aplicar l'etiquetatge d'una determinada informació caldrà tenir en compte el màxim nivell de classificació de tots els seus elements de classificació, per exemple, si part d'un document conté informació "confidencial" i altra part "reservada" caldrà etiquetar la informació com "reservada".
Qualsevol informació no etiquetada ha de considerar-se "interna".

Classificació	Etiqueta	Observació
Reservada	RESERVAT	Etiquetatge obligatori
Confidencial	CONFIDENCIAL	Etiquetatge obligatori
Interna	ÚS INTERN	Etiquetatge optatiu. Tota informació no etiquetada es considerarà d'ús intern.

Pública	ÚS PÚBLIC	Cal etiquetar-la per evidenciar que es pot fer la màxima difusió de la informació.

Taula 17-etiquetatge de la informació

L'etiquetatge de la informació dependrà del seu format:

Informació electrònica

- Comentari a l'inici del codi font.
- Part de la pantalla inicial d'una aplicació.

e-mail

- La classificació ha de quedar reflectida en l'assumpte i cos del missatge.

Documents electrònics i en paper

- La classificació ha d'aparèixer en totes les pàgines, o a les capçaleres o com a marca d'aigua en diagonal.

Elements físics

- En cas de discos, cintes, pen-drives... la classificació ha de figurar en una adhesiu visible.

f) Informació externa

La informació rebuda des de fonts externes haurà de ser classificada i etiquetada d'acord amb els criteris descrits anteriorment.

g) Llistat de distribució

La informació "confidencial" o "reservada" haurà d'incloure un llistat de distribució identificant les persones i/o departaments autoritzats a accedir-hi.

h) Distribució de la informació

La distribució de la informació haurà de fer-se d'acord amb els criteris assenyalats a la següent taula, a excepció de requeriments legals o requeriments judicials.

Classificació	Personal APZ	Prestadors de serveis	Clients	Altres
Reservada	Només a la persona o grup identificat	No autoritzat	No autoritzat	No autoritzat

Confidencial	Només a la persona o grup identificat	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació
Interna	Sense restriccions	Autoritzada, excepte indicació contrària del depositari de la informació	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 18-distribució de la informació

i) Utilització i protecció de la informació

Per a la adequada protecció de la informació és necessari que tot el personal destinatari de la informació apliqui els següents controls:

Documents impresos

Classificació	Emmagatzematge	Còpia	Enviament	Destrucció
Reservada	Custodia sota clau en caixa forta	Només amb autorització del depositari de la informació i control de la distribució de còpies	Enviament intern per carta. Certificació de l'enviament i confirmació de rebuda	Utilització de destructora de documentació
Confidencial	Custodia sota clau en caixa forta	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació	Utilització de destructora de documentació
Interna	Custodia sota clau	Només en les instal·lacions d'APZ	Només amb autorització del depositari de la informació	Contenidor de paper
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 19-política de seguretat documents impresos

A part d'aquestes mesures es requereix la retirada de documents de les impressores, copiadores, faxos... de forma immediata després de la seva utilització. La impressió de documents amb informació "confidencial" o "reservada", en una impressora compartida s'ha de fer bloquejant la impressora amb un codi personal.

No s’ha de deixar cap document amb informació “reservada” o “confidencial” sense vigilància, damunt d’una taula, encara que sigui per un període breu de temps.

Informació electrònica

Emmagatzematge i còpia

Classificació	Emmagatzematge xarxa pròpia	Emmagatzematge al cloud	Còpia en ordinador	Còpia en emmagatzematge extern
Reservada	Prohibida*	Prohibida*	Prohibida*	Prohibida*
Confidencial	Prohibida*	Prohibida*	Prohibida*	Prohibida*
Interna	En qualsevol àrea de la xarxa	Prohibida*	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 20-emmagatzematge i còpia informació electrònica

*Amb la excepció que una anàlisi del risc garanteixi la viabilitat

Transmissió de la informació dins de la organització

Classificació	**Fòrums, blogs, chats**	**e-mail**	**Cloud**	**Carpeta compartida**	**Carpeta pública**	**FTP**	**Altres medis de transmissió**
Reservada	Prohibida*	Només amb autorització del depositari de la informació i a les persones autoritzades. E-mail xifrat i certificat digital	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*

Confidencial	Prohibida*	e-mail xifrat i signat amb certificat digital	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*
Interna	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació	Solament amb autorització del depositari de la informació	Prohibida*
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 21-transmissió de la informació dins de la organització

*Amb la excepció que una anàlisi del risc garanteixi la viabilitat

Transmissió de la informació fora de la organització

Classificació	Fòrums, blogs, chats	e-mail	Cloud	Carpeta compartida	Carpeta pública	FTP	Altres medis de transmissió
Reservada	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*
Confidencial	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*	Prohibida*
Interna	Prohibida*	Solament amb autorització del depositari de la informació	Prohibida*	Prohibida*	Prohibida*	Solament amb autorització del depositari de la informació	Prohibida*
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 22-transmissió de la informació fora de la organització

*Amb la excepció que una anàlisi del risc garanteixi la viabilitat

A través de medis electrònics

Classificació	Telèfon/FAX	SMS-MMS	Infrarojos-bluetooth	Altres
Reservada	Prohibida a no ser que estigui xifrada	Prohibida	Prohibida	Prohibida
Confidencial	Prohibida a no ser que estigui xifrada	Prohibida	Prohibida	Prohibida
Interna	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació	Només amb autorització del depositari de la informació
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 23-transmissió de la informació a través de medis electrònics

Destrucció de la informació

Classificació	Destrucció d'informació a la xarxa (pròpia i cloud)	Destrucció d'informació en ordinadors	Destrucció d'informació en e-mail	Destrucció d'informació en unitats d'emmagatzematge extern
Reservada	No aplica (no es pot guardar informació reservada a un ordinador)*	No aplica (no es pot guardar informació reservada a un ordinador)*	Esborrar el missatge (assegurar que s'ha esborrat de la carpeta d'eliminats)	No aplica (no es pot guardar informació reservada a un ordinador)*
Confidencial	No aplica (no es pot guardar informació reservada a un ordinador)*	No aplica (no es pot guardar informació reservada a un ordinador)*	Esborrar el missatge (assegurar que s'ha esborrat de la carpeta d'eliminats)	No aplica (no es pot guardar informació reservada a un ordinador)*
Interna	Esborrar fitxer	Esborrar fitxer (assegurar que no es queda a la paperera de reciclatge)	Esborrar el missatge (assegurar que s'ha esborrat de la carpeta d'eliminats)	Esborrat segur del fitxer o destrucció del suport
Pública	Sense restriccions	Sense restriccions	Sense restriccions	Sense restriccions

Taula 24-destrucció de la informació

*Amb la excepció de que s'hagi autoritzat prèviament. Amb esborrat segur del fitxer amb software específic que garanteixi la seva destrucció complerta.

j) Protecció de la informació fora de la oficina

Quan la informació es trasllada fora de la APZ es pot estar sotmès a un major nivell de risc, fet pel qual cal aplicar les següents precaucions:

- Mantenir els suport d'informació controlats en tot moment.
- En entorns on no es pugui garantir un nivell raonable de confidencialitat (trens, avions, convencions, fires...) no comentar per telèfon ni en veu alta informació "reservada" ni "confidencial" ni llegir aquests tipus de documents.
- No custodiar informació "reservada" ni "confidencial" a les caixes fortes dels hotels.

k) Ús acceptable dels sistemes d'informació

Tot empleat haurà de ser conscient de quins usos contribueixen de forma eficaç a la seguretat de la informació de l'APZ i actuarà en conseqüència. En primer lloc, tots els sistemes d'informació als que se'ls facilita accés als usuaris, així com la informació de la activitat que generen i es processa en ells, son propietat de l'APZ.

Tot usuari actuarà en funció de:

Ús acceptable: l'ús dut a terme de forma responsable i racional, i conforme a les pautes dictades per la Organització, això és:

- Utilitzar les aplicacions amb finalitats professionals i d'acord amb l'activitat.
- Classificar la informació en funció de la seva naturalesa.
- Tractar amb tot rigor les dades de caràcter personal.
- Preservar la confidencialitat dels medis d'identificació i autenticació (contrasenyes, claus d'usuari, targetes identificatives...)
- Comunicar immediatament qualsevol sospita de risc per als sistemes o seguretat de la Organització.

Ús no acceptable: aquell que pugui influir negativament en la imatge i/o operativitat de l'APZ o del seu personal, o tenir conseqüències legals negatives:

- Usar els sistemes per cometre accions contràries als objectius de la Organització o la legalitat vigent.
- Tractar els actius d'informació de manera contrària a les pautes de classificació de la informació.
- Descàrrega i instal·lació de programes que no tinguin relació amb les tasques laborals, que comprometin la seguretat o puguin interrompre les comunicacions.

- Eludir l'autenticació o seguretat de qualsevol sistema, revelar claus d'accés, permetre a altres l'ús del compte personal, suplantar a una altra persona accedint o fent ús dels seus recursos.
- Realitzar canvis en la configuració del sistema (software o hardware).
- Executar qualsevol forma de monitorització de xarxa o equips que interceptin dades.
- Copiar informació relativa a empleats, activitat de la APZ o aplicacions de la seva propietat sense autorització.

l) Internet i correu electrònic

Amb la finalitat de minimitzar els riscos de la utilització de determinats protocols de connexió i serveis d'Internet, l'APZ vetllarà pel correcte funcionament dels mateixos, de tal manera que:

Normes d'accés a Internet

- Els usuaris són els únics responsables de les sessions iniciades a Internet des del seu terminal de treball.
- Es prohibeix modificar la configuració dels navegadors i activar serveis i ports sense autorització.
- No es permet l'accés, descàrrega o emmagatzematge de pàgines o continguts il·legals, imatges, sons i vídeos per a finalitats alienes a la feina, virus, codi maliciós, programes, jocs, missatgeria instantània, IRC, serveis de P2P.

Ús recomanat del correu electrònic

- Només es permet l'ús de bústies de correu electrònic proporcionades per l'APZ i el seu ús és estrictament laboral.
- Els usuaris són responsables de les activitats realitzades amb el seu compte de correu proporcionat per APZ.
- No facilitat i/o permetre la utilització del compte i/o bústia a persones no autoritzades.
- Es prohibeix la utilització d'altres màquines que no siguin les proporcionades per APZ, l'enviament de missatges amb adreces no assignades pels responsables de la institució i la manipulació de les capçaleres del correu sortint.
- El correu electrònic és una eina d'intercanvi d'informació i no de difusió.
- Es responsabilitat de l'usuari comunicar qualsevol anomalia.
- Es prohibeix l'ús del correu per propagar cartes encadenades, esquemes piramidals o similars, enviar correus a qui no vol rebre'ls, correu brossa,

enviar missatges a forums, newsgrous o llistes de distribució que comprometin la reputació de la Organització.

m) Emmagatzematge local

Amb la finalitat de garantir l'emmagatzematge de la informació en els sistemes de l'APZ, s'aconsella no usar dispositius d'emmagatzematge local, entre d'altres per les següents raons:

- Per la seva major vulnerabilitat a atacs o pèrdua de dades.
- Pel caràcter limitat del seu cicle de vida.
- Per que no es realitzen còpies de seguretat.
- Per que recuperar dades resulta molt complex o impossible.

Per tots aquest motius es recomana guardar les dades en els sistemes de xarxa desplegats per a tal finalitat.

n) Emmagatzematge portàtil

Degut a la naturalesa mòbil dels portàtils, CD, pen drives... i l'augment de les vulnerabilitats de la informació que contenen cal tenir especial consideració amb aquests tipus de dispositius.
En aquest context no es pot deixar mai desatès aquest tipus de dispositiu i no es permet emmagatzemar dades d'accés. És necessari xifrar la informació quan aquesta sigui confidencial o relativa a dades de caràcter personal.

o) Ús responsable de telèfon fix, mòbil i fax

L'APZ proporciona accés a telefonia fixa, mòbil i fax amb la finalitat d'augmentar la productivitat i millorar el desenvolupament de les activitats pròpies de la organització. L'ús fraudulent del telèfon o del fax pot posar en perill la integritat de la Institució i lesionar els seus interessos.
L'ús per finalitats personals de les comunicacions de telefonia únicament està permès si es realitza de forma fortuïta o insignificant i no interfereix en les activitats laborals habituals. Qualsevol ús personal:

- No ha de suposar cost per a la Organització.
- No ha d'estar associat a una entitat política.
- No ha de promoure l'activitat d'una altra empresa.
- No ha d'atemptar contra la reputació i nom de l'APZ.

Queda prohibit l'ús del fax i de les comunicacions telefòniques de l'APZ quan la finalitat sigui qualsevol de les descrites a continuació:

- Benefici personal.

- Negocis personals.
- Activitats polítiques personals.
- Comportament antisocial o immoral.
- Activitats que violin la legislació local, autonòmica, nacional o internacional.
- Activitats recreatives.
- Divulgació no autoritzada d'informació confidencial.
- Activitats incompatibles amb els valors propis de la Institució.
- Distribució de material inapropiat o ofensiu.

Per tots aquests motius l'APZ es reserva el dret de monitoritzar les trucades realitzades i faxos enviats, per la verificació del compliment de les seves normes i davant la sospita o evidencia d'ús fraudulent o abusiu.

p) Ús responsable de la impressora, fotocopiadora i escàner

Els recursos de reprografia, impressió i digitalització són eines de treball posades a disposició dels treballadors de l'APZ. El treballador ha d'assegurar-se que no quedin documents impresos en la safata de sortida o retinguts en la cua d'impressió que contingui dades de caràcter personal ni confidencial, així com retirar els documents conforme vagin sortint impresos. Aquest mateix comportament es produirà amb els faxos, escàner o altres dispositius d'anàloga funcionalitat.

q) Política d'escriptori net

Es crucial protegir la informació confidencial. Les oficines de l'APZ són sovint visitades per proveïdors, clients, consultors, personal de neteja i altres companys de treball.
La política d'escriptori net afecta a la informació en qualsevol format i la seva finalitat és el d'evitar que recaigui en mans no autoritzades, el que podria afectar a la imatge i reputació de la organització.
Els escriptoris o taules de treball han de romandre netes de documents de paper i dispositius d'emmagatzematge digital, especialment fora de l'horari laboral. En aquest sentit caldrà donar especial atenció amb els documents d'impressores, faxos o rebuig físic de documentació.
Es considera una bona pràctica que els empleats mantinguin el seu escriptori el més net i organitzat possible.
Durant el dia cal emmagatzemar els documents que continguin informació personal i confidencial en calaixos sota clau.
Al finalitzar la jornada laboral cal recollir i assegurar el material confidencial, tancar el despatx i els calaixos amb clau i assegurar que els equips

informàtics i qualsevol altre equip que estigui sota la seva responsabilitat estigui degudament apagat.

r) Ús de dispositius mòbils

El usuaris són els únics responsables dels equips mòbils proporcionats per a la realització de la seva feina.
En cap cas es podrà modificar la configuració del dispositiu ni instal·lar serveis no obrir ports sense autorització del responsable de seguretat.
Queda prohibida la descàrrega i emmagatzemament de:

- Pàgines o continguts il·legals, inadequats o ofensius.
- Imatges i/o vídeos amb finalitats alienes a les laborals ja que pot alentir la connexió del dispositiu amb els sistemes corporatius.
- Virus, codi maliciós, i en general, tot tipus de programes sense l'autorització del responsable de seguretat de la organització.

Queda prohibida tota utilització amb finalitats alienes a les activitats de l'APZ.

Ús segur de dispositius mòbils

Per minimitzar els riscos associats a la informació continguda al dispositiu cal implantar les següents mesures de seguretat:

- Xifrat de la informació del dispositiu.
- Canals de comunicacions segurs. Evitar la utilització de xarxes WIFI públiques ja que en molts cassos no són segures. Evitar la connexió automàtica a xarxes wifi, Bluetooth... En cas de necessitar connectivitat fer-ho a través de la connexió 3G/4G del dispositiu o a través d'una VPN proporcionada per l'APZ.
- Establir contrasenyes o PINS d'accés al dispositiu.
- Implementar un mecanisme que permeti un esborrat complert del dispositiu de forma remota.
- Realitzar còpies de seguretat periòdiques de les dades del dispositiu.
- No utilitzar el GPS del dispositiu a no ser que sigui estrictament necessari a fi i efecte de no recopilar ni enviar informació no necessària.

Referencies

Aquesta política es correspon globalment a la normativa ISO/IEC 27002.

Entrada en vigor

Aquesta política entrarà en vigor tan aviat sigui aprovada formalment

Glossari

- Un **actiu d'informació** és un conjunt de dades d'informació de negoci o suport a negoci, creats o tractats pels sistemes d'informació i que es considera necessari protegir. Exemples: informació financera, informació de recursos humans.
- Un **servei d'accés** és un o diversos mètodes processos o aplicacions que creen, accedeixen o manipulen els actius d'informació.
- Els **elements de TI** són les dependències tecnològiques, elements tecnològics tangibles que gestionen, emmagatzemen o manipulen les dades dels actius d'informació. Exemples: xarxes, servidors, ordinadors, edificis.
- El **model de dependències** és la relació entre els serveis de la activitat i els elements dels sistemes d'informació necessaris per que puguin operar.
- L'**emmagatzematge en xarxa** és desar informació en servidors locals (dins de la xarxa de la organització), disposats a tal efecte, subjectes a la política de backup i a les mesures de seguretat requerides.
- El **cloud computing** consisteix en un o diversos sistemes que permeten emmagatzemar informació en servidors remots i accedir a ells a través d'uns serveis i aplicacions que el mateix proveïdor pot proporcionar (Saas-Paas-Iass). Per a la utilització d'aquests serveis caldrà realitzar les anàlisis complertes de qüestions legals, funcionals, jurisdiccionals i contractuals pertinents.
- **Còpia en ordinador**: Sempre que s'autoritzi, es considera còpia en ordinador l'emmagatzematge en disc dur local. Aquest emmagatzematge està fora del control de la política de backup i sota la responsabilitat de l'usuari.
- **Còpia en unitats d'emmagatzematge externes**: Emmagatzematge en CD, DVD, pen-drive, disc dur extern...
- **Depositari de la informació**: Responsable intern del tractament de la informació d'acord amb les directrius establertes pel propietari depenent del seu nivell de classificació.
- **Internet**: Mètode de connexió descentralitzada de xarxes d'ordinador implementat en un conjunt de protocols que assegura que les xarxes físiques heterogènies funcionin com una única xarxa lògica a nivell mundial.
- **Protocol de comunicacions**: És un conjunt de regles que especifiquen l'intercanvi de dades i/o ordres durant la comunicació de dispositius que formen part d'una xarxa.
- **Correu brossa**: És un terme que fa referencia als missatges no sol·licitats, habitualment de tipus publicitari, enviat en quantitats massives.

- **P2P**: Xarxa informàtica entre iguals (peer to peer), que fa referència a una xarxa que no té clients ni servidors fixos, sinó que una sèrie de nodes es comporten alhora com a clients o servidors de la resta de nodes de la xarxa. Habitualment s'utilitza per l'intercanvi de fitxers.
- **IRC**: Internet Relay Chat. És un protocol de comunicacions en temps real basat en text, que permet debats entre persones o grups de persones.
- **Dispositiu mòbil**: Ordinador mida reduïda que té la capacitat de connectar-se a Internet i que pot portar a terme altres funcions. En aquesta categoria estan els smart phones i les tablets.
- **VPN**: Extensió d'una xarxa privada a Internet. En aquest cas extensió de la xarxa d'APZ a Internet.

10.2. Annex procediment d'auditories internes

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1301 Procediment d'auditories internes

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	17-10-2016	
1.1	02-11-2016	Inclusió del control de versions

Objecte

En aquest annex s'estableixen les directrius per a realitzar auditories internes del sistema de seguretat de la informació.

Àmbit d'aplicació

El procediment descrit en aquest document és d'aplicació a tot el sistema de seguretat de la informació.

Pla

El responsable del sistema de seguretat de la informació, amb periodicitat anual, crear un programa anual d'auditoria prenent en consideració l'estat i la importància dels processos i les àrees a auditar, així com els resultats d'auditories prèvies. Aquest pla d'auditoria defineix, com a mínim, l'abast de l'auditoria, la data prevista, el criteri d'auditoria i l'equip auditor i queda documentat.

Els auditors que han de dur a terme l'auditoria són sempre persones qualificades i independents del àrea/departament a auditar. Entenent:

- Qualificada: aquella persona que tingui formació en les normes de referència i sector, experiència de, com a mínim, una auditoria en el sistema de gestió de referència.
- Independent: Aquella persona que ha hagi realitzat cap dels treballs a auditar.

Realització de l'auditoria

Els auditors apliquen la seva pròpia metodologia per realitzar l'auditoria en el calendari proposat. El responsable del sistema de seguretat de la informació i l'APZ posen a la seva disposició els medis necessaris per a realitzar les següents tasques:

- Entrevistes amb el personal implicat.
- Visites a les instal·lacions.
- Observació de la feina diària del personal.
- Estudi de la documentació aplicable.

Els auditors recullen evidències objectives de conformitat o no conformitat amb els criteris d'auditoria, revisant-les i documentant-les de forma clara i precisa.

Informe d'auditoria

L'equip auditor elabora l'**informe d'auditoria** amb, com a mínim, el següent contingut:

- Dates de realització de l'auditoria.
- Nom de l'auditor o equip auditor.
- Relació de no conformitats, oportunitats de millora i punts forts.

Resolució de les NO CONFORMITATS de l'auditoria

Totes les no conformitats que apareguin en l'informe d'auditoria seran resoltes a traves del disseny i implantació de les accions correctives corresponents. Per a garantir-ho, el responsable del sistema de seguretat de la informació consulta amb el personal vinculat en la no conformitat per analitzar les causes de les no conformitats i establir les corresponents accions correctives i pla de treball.

Els responsables de l'execució de les accions correctives són els encarregats de dur a terme un control del seguiments i tancament de les accions definides.

10.3. Annex procediment de revisió

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1105 Procediment de revisió per part de la Direcció

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	17-10-2016	
1.1	02-11-2016	Inclusió del control de versions

Objectius

La revisió de les polítiques de seguretat de la informació pretén mantenir la idoneïtat, adequació i eficàcia d'aquestes, enfront dels canvis tècnics i/o organitzatius realitzats després de ser aprovada.

Qui ha de revisar les polítiques?

La potestat per revisar i fer canvis, recaurà ne la Comissió de Seguretat, essent exclusivament aquesta l'habilitada per a tal efecte.

Quan revisar les polítiques del SGSI?

Es revisaran les polítiques de seguretat en els següents casos:

- Incidents greus de seguretat.
- Canvis que afecten a la estructura de la organització.
- Auditories internes NO conformes.

10.4. Annex gestió d'indicadors

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1351 Procediment de gestió d'indicadors

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	18-10-2016	
1.1	02-11-2016	Inclusió del control de versions

Objectiu

Avaluar l'efectivitat dels controls aplicats i determinar si aquests s'ajusten als objectius de seguretat definits per l'organització.

Indicadors

INVENTARI D'ACIUS		
IDENTIFICADOR	IND01	
DEFINICIÓ		
L'identificador permet determinar el nombre d'actius de sistemes d'informació que s'han inclòs en l'inventari d'actius de seguretat de la informació.		
OBJECTIU		
Determinar el percentatge d'actius de la organització que estan correctament registrats en l'inventari d'actius de seguretat de la informació		
TIPUS D'INDICADOR	INDICADOR DE GESTIÓ	
DESCRIPCIÓ DE VARIABLES		
NOM	DESCRIPCIÓ	FONT
VAR1	Nombre d'actius de sistemes d'informació.	Informació financera sobre adquisicions d'actius de sistemes (sw/hardware).
VAR2	Nombre d'actius al registre d'actius de seguretat de la informació	Inventari d'actius de seguretat de la informació
FÓRMULA	**PERIODICITAT**	
(VAR1/VAR2)*100	TRIMESTRAL	
FITA		
VALOR > 90%		
COMENTARIS	Cal garantir que els actius de sistemes d'informació adquirits a la organització que poden ser utilitzats per emmagatzemar i tractar informació són correctament registrats en l'inventari de seguretat de la informació, encara que la informació que maneguin no sigui crítica.	

Taula 25-indicador inventari d'actius

COBERTURA DEL SGSI		
IDENTIFICADOR	IND02	
DEFINICIÓ		
L'identificador permet determinar el grau de cobertura que dóna l'SGSI als actius crítics d'informació.		
OBJECTIU		
Determinar el percentatge d'actius crítics d'informació que es troben sota el paraigües de gestió del SGSI.		
TIPUS D'INDICADOR	INDICADOR DE GESTIÓ	
DESCRIPCIÓ DE VARIABLES		
NOM	DESCRIPCIÓ	FONT
VAR3	Nombre d'actius crítics d'informació inclosos en l'abast del SGSI.	Abast del SGSI
VAR4	Nombre d'actius crítics d'informació.	Inventari d'actius
FÓRMULA		**PERIODICITAT**
(VAR1/VAR2)*100		BIANUAL
FITA		
VALOR > 90%		

Taula 26-indicador cobertura del SGSI

COST MIG DERIVAT D'UN INCIDENT DE SEGURETAT		
IDENTIFICADOR	IND03	
DEFINICIÓ		
L'identificador permet determinar el cost mig derivat d'un incident de seguretat		
OBJECTIU		
Determinar si l'objectiu de seguretat de reduir els costos associats a un incident de seguretat evoluciona satisfactòriament.		
TIPUS D'INDICADOR	INDICADOR DE CUMPLIMENT	
DESCRIPCIÓ DE VARIABLES		
NOM	DESCRIPCIÓ	FONT
VAR5	Cost de tots els incidents de seguretat	Informació financera
VAR6	Nombre d'incidents de seguretat	Seguretat de la informació
FÓRMULA		**PERIODICITAT**
(VAR5/VAR6)		ANUAL
FITA		
Encara no hi ha referències per poder establir la fita. El que cal veure es que la tendència sigui a la baixa.		

Taula 27-indicador cost mig derivat d'un incident de seguretat

PERCENTATGE DE TEMPS ONLINE DEL CONTROL D'ACCESSOS		
IDENTIFICADOR	IND04	
DEFINICIÓ		
L'identificador permet determinar el temps de disponibilitat (up time) del control d'accessos.		
OBJECTIU		
Determinar si el temps de disponibilitat del control d'accessos es correcte i determinar el temps total de no disponibilitat.		
TIPUS D'INDICADOR	INDICADOR DE CUMPLIMENT	
DESCRIPCIÓ DE VARIABLES		
NOM	DESCRIPCIÓ	FONT
VAR7	Temps de no disponibilitat	Sistemes d'informació
FÓRMULA		**PERIODICITAT**
(TEMPS TOTAL-VAR7)*100/TEMPS TORTAL		TRIMESTRAL
FITA		
Valor superior o igual a 99 %		
• Degut a la importància de mantenir en funcionament aquest sistema, és interessant definir un indicador específicament per a ell. • El temps total es el temps de 90 dies • que formen 1 trimestre.		

Taula 28-indicador percentatge de temps online del control d'accessos

GRAU DE SENSIBILITZACIÓ DEL SGSI		
IDENTIFICADOR	IND05	
DEFINICIÓ		
Capacitació, entrenament i pressa de consciència.		
OBJECTIU		
Mesurar la sensibilitat dels empleats enfront l'SGSI.		
TIPUS D'INDICADOR	INDICADOR DE CUMPLIMENT	
DESCRIPCIÓ DE VARIABLES		
NOM	DESCRIPCIÓ	FONT
VAR8	Nombre de capacitacions programades	Recursos Humans
VAR9	Nombre de capacitacions executades	Recursos Humans
FÓRMULA		**PERIODICITAT**
(VAR9/VAR8)*100		ANUAL
FITA		
Valor superior o igual a 80 %		

Taula 29-indicador grau de sensibilització del SGSI

10.5. Annex declaració d'aplicabilitat SOA

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1350 Declaració d'aplicabilitat SOA

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	20-10-2016	
1.1	02-11-2016	Inclusió del control de versions

CONTROL	APLICA	EL CONTROL ESTÀ IMPLEMENTAT?
[5] Política de seguretat		
[5.1] Política de seguretat de la informació		
[5.1.1] Document de la política de seguretat de la informació	SI	NO
[5.1.2] Revisió de la política de seguretat de la informació	SI	NO
[6] Organització de la seguretat de la informació		
[6.1] Organització interna		
[6.1.1] Compromís de la direcció amb la seguretat de la informació	SI	NO
[6.1.2] Coordinació en seguretat de la informació	SI	PARCIALMENT
[6.1.3] Assignació de responsables de seguretat de la informació	SI	SI
[6.1.4] Procés d'autorització per les instal·lacions de processament d'informació	SI	SI
[6.1.5] Acords de confidencialitat	SI	SI
[6.1.6] Contacte amb les autoritats	SI	NO
[6.1.7] Contacte amb grups d'interès	SI	SI
[6.1.8] Revisió independent de seguretat de la informació	SI	NO
[6.2] Terceres parts		
[6.2.1] Identificació del risc associat a les terceres parts	SI	NO
[6.2.2] Abordar la seguretat quan es tracta de clients	SI	NO
[6.2.3]Abordar la seguretat en acords amb terceres parts	SI	NO
[7] Gestió d'actius		
[7.1] Responsabilitat dels actius		
[7.1.1] Inventari dels actius	SI	SI
[7.1.2] Propietat dels actius	SI	PARCIALMENT
[7.1.3] Ús acceptable dels actius	SI	PARCIALMENT
[7.2] Classificació de la informació		
[7.2.1] Directives de classificació de la informació	SI	SI
[7.2.2] Etiquetatge de la informació i manipulació	SI	PARCIALMENT
[8] Seguretat dels recursos humans		
[8.1] Abans de la contractació		
[8.1.1] Rols i responsabilitats	SI	SI
[8.1.2] Screening	SI	SI
[8.1.3] Termes i condicions de la contractació	SI	SI
[8.2] Durant la contractació		
[8.2.1] Responsabilitats en la gestió	SI	NO
[8.2.2] Conscienciació, formació i entrenament en seguretat de la Informació	SI	NO
[8.2.3] Procés disciplinari	SI	SI
[8.3] Finalització o canvi d'ocupació		
[8.3.1] Finalització de responsabilitats	SI	SI
[8.3.2] Retorn dels actius	SI	SI
[8.3.3] Eliminació dels drets d'accés	SI	SI
[9] Seguretat física i ambiental		
[9.1] Zones segures		
[9.1.1] Perímetre de seguretat física	SI	SI
[9.1.2] Controls d'entrada físics	SI	SI
[9.1.3] Control d'oficines, sales i instal·lacions	SI	Si

[9.1.4] Protecció contra amenaces externes i ambientals	SI	PARCIALMENT
[9.1.5] Treballant en zones segures	SI	PARCIALMENT
[9.1.6] Zones d'accés públic, lliurament i càrrega	SI	PARCIALMENT
[9.2] Equipament de seguretat		
[9.2.1] Localització d'equips i protecció	SI	PARCIALMENT
[9.2.2] Instal·lacions de suport	SI	SI
[9.2.3] Seguretat del cablejat	SI	PARCIALMENT
[9.2.4] Manteniment d'equips	SI	SI
[9.2.5] Seguretat dels equips fora de les instal·lacions	SI	NO
[9.2.6] Eliminació o reutilització segura	SI	SI
[9.2.7]Eliminació de la propietat	SI	NO
[10] Gestió de les comunicacions i operacions		
[10.1] Procediments i responsabilitats en l'operació		
[10.1.1] Procediments d'operació documentats	SI	PARCIALMENT
[10.1.2] Gestió del canvi	SI	SI
[10.1.3] Segregació de funcions	SI	NO
[10.1.4] Separació de l'entorn de desenvolupament, test i producció	SI	PARCIALMENT
[10.2] Gestió del servei entregat per terceres parts		
[10.2.1] Entrega del servei	SI	NO
[10.2.2] Monitorització i revisió dels serveis entregats per terceres parts	SI	SI
[10.2.3] Gestió dels canvis als serveis de terceres parts	SI	SI
[10.3] Planificació i acceptació del sistema		
[10.3.1] Gestió de la capacitat	SI	PARCIALMENT
[10.3.2] Acceptació del sistema	SI	PARCIALMENT
[10.4] Protecció contra codi maliciós i mòbil		
[10.4.1] Protecció contra codi maliciós	SI	SI
[10.4.2] Protecció contra codi mòbil	SI	NO
[10.5] Backup		
[10.5.1] Backup de la informació	SI	SI
[10.6] Gestió de la seguretat de la xarxa		
[10.6.1] Controls de xarxa	SI	SI
[10.6.2] Seguretat dels serveis de xarxa	SI	SI
[10.7] Manipulació de mitjans		
[10.7.1] Gestió de mitjans extraïbles	SI	NO
[10.7.2] Destrucció de mitjans	SI	NO
[10.7.3] Procediments de manipulació de la informació	SI	NO
[10.7.4] Seguretat de la documentació del sistema	SI	SI
[10.8] Intercanvi d'informació		
[10.8.1] Procediments i polítiques d'intercanvi d'informació	SI	NO
[10.8.2] Acords d'intercanvi	SI	NO
[10.8.3] Mitjans físics en trànsit	SI	NO
[10.8.4] Missatgeria electrònica	SI	SI
[10.8.5] Sistemes d'informació empresarial	SI	PARCIALMENT
[10.9] Serveis de comerç electrònic		
[10.9.1] Comerç electrònic	NO	
[10.9.2] Transaccions on-line	NO	
[10.9.3] Informació pública disponible	SI	PARCIALMENT
[10.10] Monitorització		
[10.10.1] Auditoria de registres	SI	SI
[10.10.2] Monitorització de l'ús del sistema	SI	SI
[10.10.3] Protecció de la informació dels registres	SI	NO

[10.10.4] Registres d'administrador i d'operador	SI	SI
[10.10.5] Registre de fallades	SI	PARCIALMENT
[10.10.6] Sincronització de rellotges	SI	NO
[11] Control d'accessos		
[11.1] Requeriments empresarials pel control d'accessos		
[11.1.1] Política de control d'accessos	SI	PARCIALMENT
[11.2] Gestió d'accessos d'usuari		
[11.2.1] Registre d'usuari	SI	SI
[11.2.2] Gestió de privilegis	SI	PARCIALMENT
[11.2.3] Gestió dels passwords d'usuari	SI	SI
[11.2.4] Revisió dels privilegis d'usuari	SI	NO
[11.3] Responsabilitats d'usuari		
[11.3.1] Utilització de passwords	SI	SI
[11.3.2] Equips d'usuari desatesos	SI	NO
[11.3.3] Política de taula i pantalla neta	SI	PARCIALMENT
[11.4] Control d'accés a la xarxa		
[11.4.1] Política sobre ús de serveis de xarxa	SI	PARCIALMENT
[11.4.2] Autenticació d'usuaris per a connexions remotes	SI	SI
[11.4.3] Identificació d'equips a la xarxa	SI	NO
[11.4.4] Diagnosi remota i protecció del port de configuració	SI	PARCIALMENT
[11.4.5] Segmentació de xarxa	SI	SI
[11.4.6] Control de connexió a la xarxa	SI	SI
[11.4.7] Control d'enrutament de xarxa	SI	SI
[11.5] Control d'accés a sistemes operatius		
[11.5.1] Procediments de log on segur	SI	SI
[11.5.2] Identificació i autenticació d'usuari	SI	SI
[11.5.3] Sistema de gestió de passwords	SI	SI
[11.5.4] Ús d'utilitats del sistema	SI	PARCIALMENT
[11.5.5] Time out de sessió	SI	SI
[11.5.6] Limitació del temps de connexió	SI	NO
[11.6] Control d'accés a les aplicacions i a la informació		
[11.6.1] Restriccions d'accés a la informació	SI	SI
[11.6.2] Aïllament de sistemes sensibles	SI	PARCIALMENT
[11.7] Teletreball i mobilitat		
[11.7.1] Mobilitat i comunicacions	SI	NO
[11.7.2] Teletreball	SI	NO
[12] Adquisició de sistemes d'informació, desenvolupament i manteniment		
[12.1] Requeriments de seguretat dels sistemes d'informació		
[12.1.1] Anàlisi i especificació dels requeriments de seguretat	SI	PARCIALMENT
[12.2] Processament correcte a les aplicacions		
[12.1.1] Validació d'entrada de dades	SI	PARCIALMENT
[12.2.2] Control del processament intern	SI	NO
[12.2.3] Integritat dels missatges	SI	NO
[12.2.4] Validació de les dades de sortida	SI	NO
[12.3] Controls criptogràfics		
[12.3.1] Polítiques en l'ús de controls criptogràfics	SI	NO
[12.3.2] Gestió de claus	SI	NO
[12.4] Seguretat dels sistemes de fitxers		
[12.4.1] Control del software operacional	SI	PARCIALMENT
[12.4.2] Protecció de les dades de prova del sistema	SI	NO

[12.4.3] Control d'accés al codi font	SI	NO
[12.5] Seguretat en els processos de desenvolupament i de suport		
[12.5.1] Procediment de control de canvis	SI	NO
[12.5.2] Revisió tècnica de les aplicacions després des canvis en el sistema operatiu	SI	PARCIALMENT
[12.5.3] Restriccions en els canvis en els paquets de software	SI	NO
[12.5.4] Fuga d'informació	SI	PARCIALMENT
[12.5.5] Desenvolupament extern de software	SI	SI
[12.6] Gestió de vulnerabilitats tècniques		
[12.6.1] Control de vulnerabilitats tècniques	SI	NO
[13] Gestió d'incidents de seguretat de la informació		
[13.1] Report d'incidents de seguretat de la informació i feblesa		
[13.1.1] Report d'events de seguretat de la informació	SI	PARCIALMENT
[13.1.2] Report de febleses	SI	NO
[13.2] Gestió d'incidents de seguretat de la informació i millores		
[13.2.1] Responsabilitats i procediments	SI	NO
[13.2.2] Aprenentatge de incidents de seguretat de la informació	SI	NO
[13.2.3] Recol·lecció d'evidències	SI	NO
[14] Gestió de la continuïtat de negoci		
[14.1] Aspectes de seguretat de la informació en la gestió de la continuïtat de negoci		
[14.1.1] Inclusió de la seguretat de la informació en el procés de gestió de continuïtat de negoci	SI	NO
[14.1.2] Continuïtat de negoci i avaluació de riscos	SI	NO
[14.1.3] Desenvolupament i implementació de plans de continuïtat de negoci incloent la seguretat de la informació	SI	BO
[14.1.4] Marc de planificació de continuïtat de negoci	SI	NO
[14.1.5] Proves, manteniment, re-avaluació dels plans de continuïtat de Negoci	SI	NO
[15] Conformitat		
[15.1] Compliment amb els requeriments legals		
[15.1.1] Identificació de la legislació aplicable	SI	SI
[15.1.2] Drets de propietat intel·lectual	SI	SI
[15.1.3] Protecció del registres de la organització	SI	SI
[15.1.4] Protecció de dades y privacitat de la informació personal	SI	SI
[15.1.5] Prevenció del mal ús de les instal·lacions de processament d'informació	SI	SI
[15.1.6] Regulació dels controls criptogràfics	NO	
[15.2] Conformitat amb polítiques i estàndards de seguretat y conformitat tècnica		
[15.2.1] Conformitat amb polítiques de seguretat i estàndards	SI	NO
[15.2.2] Revisió de la conformitat tècnica	SI	PARCIALMENT

[15.3] Consideracions d'auditoria dels sistemes d'informació		
[15.3.1] Controls d'auditoria de sistemes d'informació	SI	PARCIALMENT
[15.3.2] Protecció de les eines d'auditoria de sistemes d'informació	SI	PARCIALMENT

10.6. Annex metodologia d'anàlisi de riscos

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1352 Metodologia d'anàlisi de riscos

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	18-10-2016	
1.1	02-11-2016	Inclusió del control de versions
1.2	30-11-2016	Ampliació de la descripció de la metodologia d'AR

Introducció

El Consell Superior d'Administració Electrònica (CSAE) ha creat i promou MAGERIT com a **M**etodologia d'**A**nàlisi i **G**estió de **R**iscos **IT**. Com que la Organització objecte d'aquest treball es depenent de l'administració general de l'estat és raonable pensar en utilitzar aquesta metodologia.
MAGERIT, està basada en la ISO 31000, norma no certificable però que descriu una sèrie de principis i bones pràctiques per a una correcta gestió del risc.

MAGERIT persegueix els següents objectius:

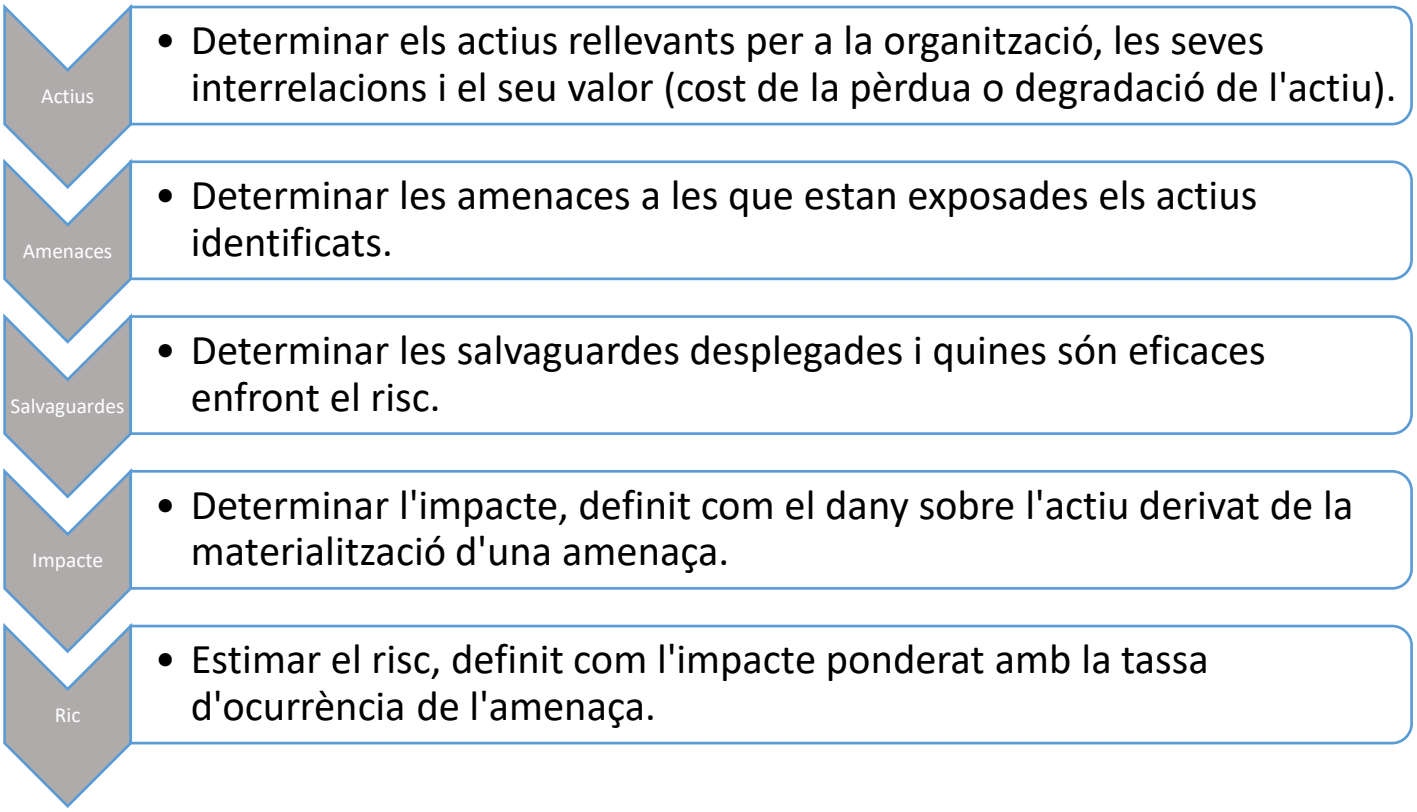
1. Conscienciar als responsables de les organitzacions de l'existència de riscos i de la necessitat de gestionar-los.
2. Oferir un mètode sistemàtic per analitzar els riscos derivats de l'ús de les tecnologies de la informació i comunicacions.
3. Ajudar a descobrir i planificar el tractament oportú per a mantenir els riscos sota control.
4. Preparar a l'organització per processos d'avaluació, auditoria, certificació o acreditació.

En la seva tercera versió, Magerit, s'ha estructurat en tres llibres: "Mètode", "Catàleg d'Elements" i "Guia de Tècniques".

A més, per a aquesta metodologia podem trobar PILAR. PILAR és una aplicació desenvolupada pel CNN (Centre Cristològic Nacional) que implementa MAGERIT, i que facilitarà el procés d'anàlisi de riscos.

Fases de la metodologia

A continuació es fa un breu resum de la metodologia Magerit 3.0. Aquesta metodologia, descrita en la documentació de MAGERIT 3 llibre I – Mètode, té quatre fases i genera una sèrie de documentació descrita a continuació.



Actius

Aquesta activitat té com a objectiu identificar els actius rellevants dintre de la organització. Aquests actius seran l'objecte d'anàlisi i cal agrupar-los per tipus d'actiu i establir les relacions i dependències entre ells. Per a cada actiu cal determinar les dimensions de la seguretat importants per a ell i quantificar la seva importància. Del resultat d'aquesta fase s'obté la següent documentació:

- Inventari i identificació dels actius a analitzar.
- Dependències entre els actius.
- Valoració dels actius.

Amenaces

Durant aquesta fase s'identifiquen les amenaces rellevants sobre el sistema objecte de l'anàlisi. Per a cada actiu (o grup d'actius) es calcula la probabilitat d'ocurrència d'una amenaça i es quantifica el dany que l'amenaça causaria en cas de materialitzar-se sobre l'actiu. Del resultat d'aquesta fase s'obté la següent documentació:

- Identificació de les amenaces per a cada actiu.
- Valoració de les amenaces.

Salvaguardes

Aquesta activitat té com a objectiu identificar les salvaguardes desplegades en el sistema objecte de l'anàlisi, qualificant-les per la seva eficàcia enfront les amenaces que es pretenen mitigar.
La documentació resultant d'aquesta fase és la següent:

- Identificació de les salvaguardes.
- Valoració de les salvaguardes.

Estimació de l'estat del risc

Amb les dades recol·lectades en els apartats anteriors es realitza el càlcul per determinar:

- Estat del risc: Que es calcula com el producte de la probabilitat que es produeixi una amenaça i l'impacte que provocaria sobre l'actiu.

La descripció completa de la metodologia es troba al Portal d'Administració Electrònica del Ministeri d'Hisenda i Administracions Públiques.

10.7. Annex procediment de rols i responsabilitats

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-1353 Procediment de rols i responsabilitats

CONTROL DOCUMENTAL	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	19-10-2016	
1.1	02-11-2016	Inclusió del control de versions

Objectiu

Descriure l'estructura de personal que composa el comitè de seguretat de l'organització.

Comitè de seguretat de la informació

És necessari crear un comitè de seguretat de la informació que tingui responsabilitat directa sobre la seguretat de la informació. Aquesta estructura de personal ha de tenir clarament definida les seves responsabilitats i funcions. Per garantir el compromís de l'alta direcció de l'organització és necessari que part d'aquest comitè estigui format per membre del comitè executiu de l'organització. També ha de formar part d'aquest comitè els caps de departament propietaris de la informació crítica per a l'organització.
A més, pel l'èxit del SGSI és necessari que l'alta direcció doti dels recursos econòmics, tècnics i humans necessaris per al correcte desenvolupament de les funcions del comitè.
Funcions principals d'aquest comitè:

- Dotar del suport de les autoritats de la organització a les iniciatives de seguretat de la informació.
- Aprovar la estratègia, polítiques, directrius, normes i procediments de seguretat de la informació.
- Determinar les responsabilitats de tot el personal involucrat.
- Promoure una cultura de seguretat de la informació en la organització.

Composició del comitè

- Director General de l'organització.
- Director de Sistemes d'Informació, també amb el seu rol de CISO de l'organització.
- Director de Seguretat Industrial, també amb el seu rol de responsable del sistema de control d'accessos al recinte portuari.
- Director d'Operacions Portuàries com a responsable del sistema Port Community System.
- Director d'Administració i Finances com a responsable del sistema Integra II i de l'ERP financer.
- Directora de Secretaria General i Serveis Jurídics com a responsable de l'Administració Electrònica i compliment legal de la companyia.
- Responsable de Qualitat del Departament de Sistemes d'Informació.

El comitè de seguretat pot requerir, quan ho cregui oportú pel correcte exercici de les seves funcions, la participació d'altres treballadors de l'organització o empreses terceres que li donin suport.

Director de seguretat de la informació

- Establir i mantenir una estratègia de seguretat de la informació alineada amb les fites i objectius de l'organització.
- Establir i mantenir un marc de referencia del govern de seguretat de la informació per orientar les activitats que donin suport a l'estratègia de seguretat de la informació.
- Integrar el govern de la seguretat de la informació dins del govern corporatiu.
- Establir i mantenir polítiques de seguretat de la informació. Comunicar les directrius als gerents i orientar el desenvolupament de normes, procediments i pautes.
- Integrar el govern de la seguretat de la informació dins del govern corporatiu.
- Establir i mantenir polítiques de seguretat de la informació. Orientar en el desenvolupament de normes, procediments i pautes.
- Establir, supervisar, avaluar i reportar les mesures.
- Establir i mantenir un procés de classificació d'actius d'informació.
- Identificar requeriments legals, reglamentaris, organitzatius i altres aplicables per a gestionar el risc de incompliment a nivells acceptables.
- Establir un procés d'avaluació de riscos i vulnerabilitats i vetllar pel seu correcte funcionament.
- Avaluar els controls de seguretat per determinar si són apropiats i en efecte mitiguen el risc a un nivell acceptable.
- Identificar els nivells actuals de risc i els desitjats.
- Assegurar un procés de gestió del risc integral dintre de l'organització.
- Supervisar la gestió del canvi en els actius d'informació per assegurar que els nous nivells de risc són acceptables i en cas contrari revaluar les mesures.
- Informar del incompliment.
- Establir, mantenir i comunicar els estàndards, procediments i guies i altres documents de seguretat de la informació.
- Establir i mantenir un programa de conscienciació i capacitació de la seguretat de la informació.
- Integrar els requeriments de seguretat de la informació dins els processos de la organització.
- Establir un sistema per avaluar la eficàcia del programa de seguretat de la informació.

- Establir i mantenir i desenvolupar un pla de resposta i recuperació a incidents de seguretat de la informació així com la seva categorització i identificació d'incidents de seguretat.

10.8. Annex valoració d'actius

CLASSE	ID	ACTIU	VALOR	C	I	D	A	T	DEPENDÈNCIES
[L]	L1	Data Center Principal APZ	MA	9	9	10	10	9	
	L2	Sala tècnica 1	MA	9	9	10	10	9	
	L3	Sala tècnica 2	MA	9	9	10	10	9	
	L4	Sala tècnica 3	MA	9	9	10	10	9	
	L5	Despatx tècnics d'operacions	A	1	9	7	10	9	
	L6	Sala tècnica control d'accessos	MA	9	9	10	10	9	
	L7	Despatx tècnics emergències	A	5	8	10	7	10	
[HW]	HW1	Clúster de 6 servidors	MA	9	9	10	9	9	L1,COM1,AUX1,AUX6
	HW2	Cabina de discos	MA	9	9	10	9	9	L1,COM1,AUX1,AUX6
	HW3	10 Ordinadors tècnics operacions	A	5	8	8	9	9	L5,COM1,AUX11
	HW4	5 Ordinadors tècnics emergències	A	5	7	10	9	10	L7,COM1, COM2,AUX11
	HW5	Core de comunicacions	A	8	7	10	9	9	L1,AUX1,AUX6,AUX12
	HW6	Pila switch L2	A	8	7	10	8	8	L2, AUX2, AUX7,AUX12
	HW7	Pila switch L3	A	8	7	10	8	8	L3,AUX3,AUX8,AUX12
	HW8	Pila switch L5	A	8	7	10	8	8	L5,AUX5, AUX9,AUX12
	HW9	Servidors de telefonia	MA	5	7	10	9	10	L1,COM1,COM2,AUX1,AUX6,AUX12
	HW10	Telèfons tècnics emergències	A	5	7	10	9	10	L7,COM1, COM2,AUX11,AUX12
[SW]	SW1	Windows Server (Diversos)	MA	9	9	10	9	9	HW1,HW2
	SW2	Windows Exchange	B	5	5	7	5	5	HW1,HW2
	SW3	SQL Server	MA	9	9	10	9	9	HW1,HW2

	SW4	Microsoft Dynamics	M	8	9	6	10	7	HW1,HW2
	SW5	Port Community System	MA	5	9	10	9	9	HW1,HW2
	SW6	Administració electrònica	B	10	10	7	10	10	HW1,HW2
	SW7	Control d'accessos	MA	10	8	10	10	10	HW1,HW2
	SW8	CISCO Call Manager	MA	5	7	10	9	10	HW9
	SW9	Integra II	A	5	9	7	9	9	HW1,HW2
	SW10	JBOSS	MA	5	9	10	9	9	HW1,HW2
	SW11	Microsoft IIS	MA	5	9	7	9	9	HW1,HW2
	SW12	Microsoft ISA Server	B	5	7	7	5	5	HW1,HW2
	SW13	Microsoft Windows 7	A	5	7	10	7	10	HW3, HW4
	SW14	Gestió d'emergències	A	5	7	10	10	10	HW1,HW2
[D]	D1	Dades generades pel PCS	MA	5	9	10	9	9	HW1,HW2,SW5,SW11,SW3,SW12,COM1
	D2	Dades generades per IntegraII	A	5	9	7	9	9	HW1,HW2,SW9,SW10,SW3,SW10
	D3	Dades generades per Administració Electrònica	B	10	10	7	10	10	HW1,HW2,SW6,SW10,SW3,SW10,COM1
	D4	Dades de caràcter personal	MA	10	10	5	10	10	HW1,HW2,SW7,SW5,SW6,SW7,SW3,SW4
	D5	Dades confidencials	MA	10	10	5	10	10	HW1,HW2,SW7,SW5,SW6,SW7,SW3,SW4
	D6	Dades generades per Dynamics	M	8	9	6	10	7	HW1,HW2,SW4
	D7	Dades generades pel control d'accessos	MA	10	8	10	10	10	HW1,HW2,SW7
	D8	Dades de trucades d'emergències (logs i enregistraments)	MA	5	7	10	9	10	HW9, SW8, COM1,COM2,AUX12
[COM]	COM1	Accés a Internet Metrolan	A	5	9	10	9	9	L1,AUX1,AUX6
	COM2	2 primaris de telefonia	MA	5	7	10	9	10	L1,AUX1,AUX6
[AUX]	AUX1	Climatització L1	MA	1	1	10	9	1	L1
	AUX2	Climatització L2	MA	1	1	10	9	1	L2
	AUX3	Climatització L3	MA	1	1	10	9	1	L3

	AUX4	Climatització L4	MA	1	1	10	9	1	L4
	AUX5	Climatització L6	MA	1	1	10	9	1	L6
	AUX6	Subministrament elèctric L1	MA	1	1	10	9	1	L1
	AUX7	Subministrament elèctric L2	MA	1	1	10	9	1	L2
	AUX8	Subministrament elèctric L3	MA	1	1	10	9	1	L3
	AUX9	Subministrament elèctric L4	MA	1	1	10	9	1	L4
	AUX10	Subministrament elèctric PCs	M	1	1	10	9	1	L5,L7
	AUX11	Subministrament elèctric edifici d'oficines.	A	1	1	10	9	1	L5,L7,L1
	AUX12	Cablejat de xarxa	MA	1	1	10	9	1	L1,L2,L3,L4,L5,L6,L7
[P]	P1	Tècnics d'operacions	MA			5			
	P2	Tècnics d'emergències	MA			5			

Taula 30-valoració d'actius

10.9. Annex valoració d'amenaces

L datacenter

Segons MAGERIT v3, aquests tipus d'actiu es pot veure afectat per: N.1, N.2, N.*, I.1, I.2, I.*, I.11, E.15, E.18, E.19, A.7, A.11, A.15, A.18, A.19, A.26, A.27

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
L1	N.1	FMB			100%		
	N.2	FB			100%		
	N.*	FMB			100%		
	I.1	FB			100%		
	I.2	FB			100%		
	I.*	FM			100%		
	I.11	FM	20%				
	E.15	FB		50%			
	E.19	FB	50%				
	A.7	FMB	20%	20%	20%		
	A.11	FMB	20%	100%			
	A.15	FB		100%			
	A.18	FMB		100%			
	A.19	FMB	20%				
	A.26	FMB			100%		
			50%	100%	100%		

Taula 31-valoració d'amenaces datacenter

L Sala tècnica

Aquests tipus d'actiu es pot veure afectat per: N.1, N.2, N.*, I.1, I.2, I.*, I.11, E.15, E.18, E.19, A.7, A.11, A.15, A.18, A.19, A.26, A.27

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
L2 L3 L4 L6	N.1	FMB			100%		
	N.2	FMB			100%		
	N.*	FMB			100%		
	I.1	FMB			100%		
	I.2	FMB			100%		
	I.*	FMB			100%		
	I.11	FMB	20%				
	E.15	FM		10%			
	E.19	FM	10%				
	A.7	FMB	10%	10%	10%		
	A.11	FMB	20%	20%			
	A.15	FMB		100%			
	A.18	FMB		100%			
	A.19	FMB	20%				
	A.26	FMB			100%		
			20%	20%	100%		

Taula 32-valoració d'amenaces sala tècnica

L oficines

Aquests tipus d'actiu es pot veure afectat per: N.1, N.2, N.*, I.1, I.2, I.*, I.11, E.15, E.18, E.19, A.7, A.11, A.15, A.18, A.19, A.26, A.27

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
L5 L7	N.1	FMB			100%		
	N.2	FMB			100%		
	N.*	FMB			100%		
	I.1	FM			100%		
	I.2	FB			100%		
	I.*	FM			100%		
	I.11	FM	20%				
	E.15	FB		10%			
	E.19	FB	10%				
	A.7	FA	10%	10%	10%		
	A.11	FM	20%	20%			
	A.15	FM		100%			
	A.18	FM		100%			
	A.19	FM	20%				
	A.26	FM			100%		
			20%	100%	100%		

Taula 33-valoració d'amenaces oficines

SW servidors

Aquests tipus d'actiu es pot veure afectat per: I.5, E.1, E.2, E.8, E.9, E.10, E.15, E.18, E.19, E.20, E.21, A.5, A.6, A.7, A.8, A.9, A.10, A.11 A.15, A.19, A.22

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
SW1 SW2 SW3 SW4 SW5 SW6 SW7 SW8 SW9 SW10 SW11 SW12 SW14	I.5	FMB			100%		
	E.1	FMB	20%	20%	20%		
	E.2	FMB	20%	50%	100%		
	E.8	FMB	20%	20%	20%		
	E.9	FMB	10%				
	E.10	FMB		20%			
	E.15	FB		10%			
	E.18	FMB			50%		
	E.19	FM	20%				
	E.20	FA	20%	20%	20%		
	E.21	FB		20%	20%		
	A.5	FB	20%	20%		100%	
	A.6	FM	20%	20%	100%		
	A.7	FB	10%	10%	10%		
	A.8	FM	20%	20%	20%		
	A.9	FMB	20%				
	A.10	FMB		20%			
	A.11	FMB	20%	20%			
	A.15	FMB		20%			

	A.18	FMB			20%		
	A.19	FMB	20%				
	A.22	FMB	20%	20%	20%		
			20%	50%	100%	100%	

Taula 34-valoració amenaces SW servidors

SW usuari

Aquests tipus d'actiu es pot veure afectat per: I.5, E.1, E.2, E.8, E.9, E.10, E.15, E.18, E.19, E.20, E.21, A.5, A.6, A.7, A.8, A.9, A.10, A.11 A.15, A.19, A.22

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
SW13	I.5	FB			100%		
	E.1	FM	10%	10%	10%		
	E.2	FM	10%	10%	100%		
	E.8	FB	20%	20%	20%		
	E.9	FMB	10%				
	E.10	FMB		20%			
	E.15	FM		10%			
	E.18	FMB			50%		
	E.19	FM	20%				
	E.20	FA	20%	20%	20%		
	E.21	FM		20%	20%		
	A.5	FB	20%	20%		100%	
	A.6	FM	20%	20%	100%		
	A.7	FB	10%	10%	10%		
	A.8	FM	20%	20%	20%		
	A.9	FMB	20%				
	A.10	FMB		20%			
	A.11	FMB	20%	20%			
	A.15	FB		20%			
	A.18	FB			20%		
	A.19	FB	20%				
	A.22	FB	20%	20%	20%		
			20%	20%	100%	100%	

Taula 35-valoració amenaces SW usuari

HW servidor

Aquests tipus d'actiu es pot veure afectat per: N.1, N.2,N.*, I.1, I.2, I.*, I.3,I.4,I.5,I.6,I.7,E.2,E.23,E.24,E.25,A.6,A.7,A.11,A.23,A.24,A.25,A.26

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
HW1 HW2 HW5 HW9	N.1	FMB			100%		
	N.2	FB			100%		
	N.*	FMB			100%		
	I.1	FB			100%		
	I.2	FB			100%		
	I.*	FM			100%		
	I.3	FM			100%		
	I.4	FMB			100%		

	I.5	FB			100%		
	I.6	FB			100%		
	I.7	FB			50%		
	E.2	FB	10%	10%	100%		
	E.23	FB			100%		
	E.24	FMB			100%		
	E.25	FMB	20%		100%		
	A.6	FMB	20%	20%	100%		
	A.7	FMB	10%	10%	10%		
	A.11	FMB	20%	20%			
	A.23	FMB	20%		10%		
	A.24	FMB			50%		
	A.25	FMB	10%		100%		
	A.26	FMB			100%		
			20%	20%	100%		

Taula 36-valoració amenaces HW servidor

HW sala tècnica

Aquests tipus d'actiu es pot veure afectat per: N.1, N.2,N.*, I.1, I.2, I.*, I.3,I.4,I.5,I.6,I.7,E.2,E.23,E.24,E.25,A.6,A.7,A.11,A.23,A.24,A.25,A.26

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
HW6 HW7 HW8	N.1	FMB			100%		
	N.2	FMB			100%		
	N.*	FMB			100%		
	I.1	FMB			100%		
	I.2	FMB			100%		
	I.*	FMB			100%		
	I.3	FM			100%		
	I.4	FM			100%		
	I.5	FB			100%		
	I.6	FM			100%		
	I.7	FM			50%		
	E.2	FB	10%	10%	100%		
	E.23	FB			100%		
	E.24	FMB			100%		
	E.25	FMB	20%		100%		
	A.6	FMB	20%	20%	100%		
	A.7	FB	10%	10%	10%		
	A.11	FB	20%	20%			
	A.23	FB	20%		10%		
	A.24	FMB			50%		
	A.25	FB	10%		100%		
	A.26	FMB			100%		
			20%	20%	100%		

Taula 37-valoració amenaces HW sala tècnica

HW usuari

Aquests tipus d'actiu es pot veure afectat per: N.1, N.2,N.*, I.1, I.2, I.*, I.3,I.4,I.5,I.6,I.7,E.2,E.23,E.24,E.25,A.6,A.7,A.11,A.23,A.24,A.25,A.26

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
HW3 HW4 HW10	N.1	FMB			100%		
	N.2	FMB			100%		
	N.*	FMB			100%		
	I.1	FMB			100%		
	I.2	FMB			100%		
	I.*	FMB			100%		
	I.3	FMB			100%		
	I.4	FMB			100%		
	I.5	FB			50%		
	I.6	FMB			100%		
	I.7	FMB			50%		
	E.2	FB	10%	10%	20%		
	E.23	FB			50%		
	E.24	FMB			50%		
	E.25	FMB	20%		50%		
	A.6	FMB	20%	20%	50%		
	A.7	FB	10%	10%	10%		
	A.11	FMB	20%	20%			
	A.23	FB	20%		10%		
	A.24	FMB			50%		
	A.25	FMB	10%		50%		
	A.26	FMB			50%		
			20%	20%	100%		

Taula 38-valoració amenaces HW usuari

COM

Aquests tipus d'actiu es pot veure afectat per: I.8, E.2, E.9, E.10, E.15, E.18, E.19, E.24, A.5, A.6, A.7, A.9, A.10, A.11, A.12, A.14, A.15, A.19, A.24

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
COM1 COM2	I.8	FMB			100%		
	E.2	FB	20%	20%	100%		
	E.9	FMB	20%				
	E.10	FMB		20%			
	E.15	FMB		20%			
	E.18	FB			100%		
	E.19	FB	20%				
	E.24	FMB			100%		
	A.5	FB	100%	20%		100%	
	A.6	FB	20%	20%	50%		
	A.7	FB	10%	10%	10%		
	A.9	FB	100%				
	A.10	FB		100%			
	A.11	FMB	20%	20%			

	A.12	FB	100%				
	A.14	FB	100%				
	A.15	FMB		100%			
	A.19	FB	20%				
	A.24	FMB			100%		
			100%	100%	100%	100%	

Taula 39-valoració amenaces COM

Dades

Aquest tipus d'actiu es pot veure afectat per: E.1, E.2, E.15, E.18, E.19, A.5, A.6, A.11, A.15, A.18, A.19

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
D1 D2 D3 D4 D5 D6 D7 D8	E.1	FB	10%	100%	10%		
	E.2	FMB	100%	100%	10%		
	E.15	FB		100%			
	E.18	FMB			100%		
	E.19	FMB	20%				
	A.5	FMB	20%	20%		100%	
	A.6	FMB	10%	10%	10%		
	A.11	FMB	100%	50%			
	A.15	FMB		100%			
	A.18	FMB			100%		
	A.19	FB	20%				
			100%	100%	100%	100%	

Taula 40-valoració amenaces Dades

Persones

Aquest tipus d'actiu es pot veure afectat per: E.7, E.19, A.28, A.29, A.30

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
P1 P2	E.7	FM			20%		
	E.19	FB	100%				
	A.28	FM			20%		
	A.29	FMB	100%	20%	20%		
	A.30	FMB	100%	20%	10%		
			100%	20%	20%		

Taula 41-valoració amenaces Persones

AUX clima

Aquest tipus d'actiu es pot veure afectat per: N*, I.1,I.2,I.*,I.3,I.4,I.5,I.6,I.7,I.9,E.23,E.25,A.7,A.11,A.23,A.25,A.26

ID actiu	ID amenaça	FREQUÈNCIA	C	I	D	A	T
AUX1	N.*	FMB			100%		
AUX2	I.1	FB			100%		
AUX3	I.2	FMB			100%		

AUX4 AUX5 AUX6 AUX7 AUX8 AUX9 AUX10 AUX11 AUX12	I.3	FB			50%		
	I.4	FB			50%		
	I.5	FB			100%		
	I.6	FB			100%		
	I.7	FB			100%		
	I.9	FMB			100%		
	E.23	FB			100%		
	E.25	FMB			100%		
	A.7	FMB			20%		
	A.11	FMB			10%		
	A.23	FMB			100%		
	A.25	FMB			100%		
	A.26	FMB			100%		
					100%		

Taula 42-valoració amenaces AUX clima

10.10. Annex impacte potencial

CLASSE	ID	VALOR	VALOR DE L'ACTIU					IMPACTE					IMPACTE POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[L]	L1	MA	9	9	10	10	9	50%	100%	100%			4,5	9	10	0	0
	L2	MA	9	9	10	10	9	20%	20%	100%			1,8	1,8	10	0	0
	L3	MA	9	9	10	10	9	20%	20%	100%			1,8	1,8	10	0	0
	L4	MA	9	9	10	10	9	20%	20%	100%			1,8	1,8	10	0	0
	L5	A	1	9	7	10	9	20%	100%	100%			0,2	9	7	0	0
	L6	MA	9	9	10	10	9	20%	20%	100%			1,8	1,8	10	0	0
	L7	A	5	8	10	7	10	20%	20%	100%			1	1,6	10	0	0
[HW]	HW1	MA	9	9	10	9	9	20%	20%	100%			1,8	1,8	10	0	0
	HW2	MA	9	9	10	9	9	20%	20%	100%			1,8	1,8	10	0	0
	HW3	A	5	8	8	9	9	20%	20%	100%			1	1,6	8	0	0
	HW4	A	5	7	10	9	10	20%	20%	100%			1	1,4	10	0	0
	HW5	A	8	7	10	9	9	20%	20%	100%			1,6	1,4	10	0	0
	HW6	A	8	7	10	8	8	20%	20%	100%			1,6	1,4	10	0	0
	HW7	A	8	7	10	8	8	20%	20%	100%			1,6	1,4	10	0	0
	HW8	A	8	7	10	8	8	20%	20%	100%			1,6	1,4	10	0	0
	HW9	MA	5	7	10	9	10	20%	20%	100%			1	1,4	10	0	0
	HW10	A	5	7	10	9	10	20%	20%	100%			1	1,4	10	0	0
[SW]	SW1	MA	9	9	10	9	9	20%	50%	100%	100%		1,8	4,5	10	9	0
	SW2	B	5	5	7	5	5	20%	50%	100%	100%		1	2,5	7	5	0
	SW3	MA	9	9	10	9	9	20%	50%	100%	100%		1,8	4,5	10	9	0

	SW4	M	8	9	6	10	7	20%	50%	100%	100%		1,6	4,5	6	10	0
	SW5	MA	5	9	10	9	9	20%	50%	100%	100%		1	4,5	10	9	0
	SW6	B	10	10	7	10	10	20%	50%	100%	100%		2	5	7	10	0
	SW7	MA	10	8	10	10	10	20%	50%	100%	100%		2	4	10	10	0
	SW8	MA	5	7	10	9	10	20%	50%	100%	100%		1	3,5	10	9	0
	SW9	A	5	9	7	9	9	20%	50%	100%	100%		1	4,5	7	9	0
	SW10	MA	5	9	10	9	9	20%	50%	100%	100%		1	4,5	10	9	0
	SW11	MA	5	9	7	9	9	20%	50%	100%	100%		1	4,5	7	9	0
	SW12	B	5	7	7	5	5	20%	50%	100%	100%		1	3,5	7	5	0
	SW13	A	5	7	10	7	10	20%	20%	100%	100%		1	3,5	10	7	0
	SW14	A	5	7	10	10	10	20%	50%	100%	100%		1	3,5	10	10	0
[D]	D1	MA	5	9	10	9	9	100%	100%	100%	100%		5	9	10	9	0
	D2	A	5	9	7	9	9	100%	100%	100%	100%		5	9	7	9	0
	D3	B	10	10	7	10	10	100%	100%	100%	100%		10	10	7	10	0
	D4	MA	10	10	5	10	10	100%	100%	100%	100%		10	10	5	10	0
	D5	MA	10	10	5	10	10	100%	100%	100%	100%		10	10	5	10	0
	D6	M	8	9	6	10	7	100%	100%	100%	100%		8	9	6	10	0
	D7	MA	10	8	10	10	10	100%	100%	100%	100%		10	8	10	10	0
	D8	MA	5	7	10	9	10	100%	100%	100%	100%		5	7	10	9	0
[COM]	COM1	A	5	9	10	9	9	100%	100%	100%	100%		5	9	10	9	0
	COM2	MA	5	7	10	9	10	100%	100%	100%	100%		5	7	10	9	0
[AUX]	AUX1	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX2	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX3	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX4	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX5	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX6	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX7	MA	1	1	10	9	1			100%			0	0	10	0	0

	AUX8	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX9	MA	1	1	10	9	1			100%			0	0	10	0	0
	AUX10	M	1	1	10	9	1			100%			0	0	10	0	0
	AUX11	A	1	1	10	9	1			100%			0	0	10	0	0
	AUX12	MA	1	1	10	9	1			100%			0	0	10	0	0
[P]	P1	MA	5	5	8			100%	20%	20%					1		
	P2	MA			5			100%	20%	20%					1		

Taula 43-impacte potencial

10.11. Annex risc residual

CLASSE	ID	VALOR	F	IMPACTE POTENCIAL					RISC				
				C	I	D	A	T	C	I	D	A	T
[L]	L1	MA	FM	4,5	9	10	0	0	4,5	9	10	0	0
	L2	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L3	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L4	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L5	A	FA	0,2	9	7	0	0	2	90	70	0	0
	L6	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L7	A	FA	1	1,6	10	0	0	10	16	100	0	0
[HW]	HW1	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	HW2	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	HW3	A	FB	1	1,6	8	0	0	0,1	0,16	0,8	0	0
	HW4	A	FB	1	1,4	10	0	0	0,1	0,14	1	0	0
	HW5	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW6	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW7	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW8	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW9	MA	FM	1	1,4	10	0	0	1	1,4	10	0	0
	HW10	A	FB	1	1,4	10	0	0	0,1	0,14	1	0	0
[SW]	SW1	MA	FA	1,8	4,5	10	9	0	18	45	10	90	0
	SW2	B	FA	1	2,5	7	5	0	10	25	70	50	10
	SW3	MA	FA	1,8	4,5	10	9	0	18	45	100	90	18
	SW4	M	FA	1,6	4,5	6	10	0	16	45	60	100	16
	SW5	MA	FA	1	4,5	10	9	0	10	45	100	90	10
	SW6	B	FA	2	5	7	10	0	20	50	70	100	20
	SW7	MA	FA	2	4	10	10	0	20	40	100	100	20
	SW8	MA	FA	1	3,5	10	9	0	10	35	100	90	10
	SW9	A	FA	1	4,5	7	9	0	10	45	70	90	10
	SW10	MA	FA	1	4,5	10	9	0	10	45	100	90	10
	SW11	MA	FA	1	4,5	7	9	0	10	45	70	90	10
	SW12	B	FA	1	3,5	7	5	0	10	35	70	50	10
	SW13	A	FA	1	3,5	10	7	0	10	35	100	70	10
	SW14	A	FA	1	3,5	10	10	0	10	35	100	100	10
[D]	D1	MA	FB	5	9	10	9	0	0,5	0,9	1	0,9	0,5
	D2	A	FB	5	9	7	9	0	0,5	0,9	0,7	0,9	0,5
	D3	B	FB	10	10	7	10	0	1	1	0,7	1	1
	D4	MA	FB	10	10	5	10	0	1	1	0,5	1	1
	D5	MA	FB	10	10	5	10	0	1	1	0,5	1	1
	D6	M	FB	8	9	6	10	0	0,8	0,9	0,6	1	0,8
	D7	MA	FB	10	8	10	10	0	1	0,8	1	1	1

	D8	MA	FB	5	7	10	9	0	0,5	0,7	1	0,9	0,5
[COM]	COM1	A	FB	5	9	10	9	0	0,5	0,9	1	0,9	0
	COM2	MA	FB	5	7	10	9	0	0,5	0,7	1	0,9	0
[AUX]	AUX1	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX2	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX3	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX4	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX5	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX6	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX7	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX8	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX9	MA	FB	0	0	10	0	0	0	0	1	0	0
	AUX10	M	FB	0	0	10	0	0	0	0	1	0	0
	AUX11	A	FB	0	0	10	0	0	0	0	1	0	0
	AUX12	MA	FB	0	0	10	0	0	0	0	1	0	0
[P]	P1	MA	FM			1			0	0	1	0	0
	P2	MA	FM			1			0	0	1	0	0

Taula 44-risc residual

10.12. Annex propostes de millora

Nom	**Pla de formació i conscienciació en matèria de seguretat de la informació**					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-01	0	2/1/2017	1 any	RRHH	Comitè de seguretat	10.000€
Objectius	• Executar un pla de formació i conscienciació per a tots els empleats de la Organització. • Mantenir un grau de conscienciació raonable en matèria de seguretat de la informació. • Afavorir que el treballador reporti incidents de seguretat quan els detecti.					
Descripció	• Sessions formatives segmentades per col·lectius de l'organització en funció de la seva responsabilitat. • Elaboració de manuals de bones pràctiques, guies, propagandes i publicacions a la intranet de la Organització per generar consciència en matèria de seguretat de la informació. • Hi haurà sessions dedicades per al personal de sistemes, sobre protecció de sistemes, pràctiques de programació segura, defensa contra atacs, vulnerabilitats, mesures de control...					
Indicadors	• Nombre d'accions formatives realitzades. • Nombre d'incidents de seguretat reportat pels treballadors.					

Taula 45-millora pla de formació

Nom	Definició de l'estructura de seguretat de la organització					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-02	0	1/1/2017	2 meses	Organització	Comitè de seguretat	Projecte intern
Objectius	• Adaptar l'estructura organitzativa per tal de crear un marc de seguretat.					
Descripció	• Definir i establir l'estructura organitzativa de seguretat de la informació de l'Organització. Definir el comitè de seguretat, membres, competències i normes de funcionament. • Definir els processos de gestió de la seguretat.					

Taula 46-millora definició de l'estructura de seguretat

Nom	Assignació i classificació dels actius d'informació					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-03	0	1/3/2017	3 mesos	Organització i responsable de seguretat	Comitè de seguretat	Projecte intern
Objectius	• Assignar propietaris i responsabilitats als actius de la Organització. • Identificar els actius d'informació crítics per a la Organització. • Establir objectius i responsabilitats vers els responsables dels actius.					
Descripció	El pla director de seguretat de la informació s'ha impulsat des de sistemes d'informació amb el suport de la direcció i s'han seleccionat els actius crítics d'informació que des del punt de vista de sistemes d'informació donen suport al negoci i el manteniment de la seva seguretat (en totes les dimensions) és crític. És necessari assignar responsables als actius que donen suport als processos de negoci i d'aquesta forma calcular el valor real i la el grau de criticitat per a la Organització.					
Indicadors	• Percentatge d'actius amb propietari.					
Dependències	• SI-PM-02					

Taula 47-millora assignació i classificació dels actius d'informació

Nom	**Elaboració d'un pla de continuïtat de negoci i resposta a incidents de seguretat**					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-04	0	10/1/2018	3 mesos	Responsable de seguretat	Comitè de seguretat	30.000 €
Objectius	• Elaboració i documentació dels procediments necessaris per garantir la continuïtat dels sistemes que donen suport a les operacions core de negoci. • Minimitzar l'impacte d'una interrupció en la continuïtat de les operacions. • Millorar la imatge de la Organització. • Establir procediments per donar una resposta adequada als incidents de seguretat					
Descripció	En l'anàlisi de riscos s'ha posat de manifest que el principal focus d'atenció cal posar-lo en garantir la disponibilitat dels sistemes. Definició del pla per protegir els principals actius de negoci a tracés d'un conjunt de tasques que permetin a la Organització recuperar-se d'un incident greu de seguretat en un termini que no comprometi la continuïtat del negoci. Establir els mecanismes per gestionar, reportar, documentar els incidents de seguretat, així com millorar el procés un cop realitzat l'anàlisi dels mateixos. D'aquest pla se'n derivaran accions concretes per implementar-ho.					
Dependències	• SI-PM-03					

Taula 48-millora elaboració pal continuïtat

Nom	Implementació de mecanisme de validació de doble factor.					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-05	0	1/6/2017	6 mesos	Responsable de seguretat. Responsable de SI	Comitè de seguretat	100.000 €
Objectius	• Assegurar l'autenticitat de la informació introduïda en els sistemes crítics per al negoci.					
Descripció	Implementar un mecanisme de doble factor per reforçar l'autenticitat de les dades introduïdes en els sistemes crítics. A més d'adquirir el servidor de tokens i les seves llicencies, el projecte inclou la modificació de les aplicacions de negoci a fi i efecte de que permetin la validació de l'usuari amb doble factor.					
Indicadors	• Percentatge d'aplicacions de negoci que permeten el doble factor.					

Taula 49-millora doble factor

Nom	Reforç dels mecanismes de protecció elèctric de les instal·lacions.					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-06	0	2/1/2017	1 mes	Responsable de seguretat. Responsable d'instal·lacions	Comitè de seguretat	60.000 €
Objectius	• Garantir la continuïtat de les instal·lacions en cas de caiguda de subministrament elèctric.					
Descripció	Adquirir sistemes d'alimentació ininterrompuda, grups electrògens i sistemes necessaris de reforç per assegurar que les instal·lacions de procés de dades no es queden sense subministrament elèctric. Els sistemes auxiliars han de poder-se monitoritzar i avisar en cas de funcionament anòmal del subministrament elèctric.					
Indicadors	• Percentatge d'aplicacions de procés de dades amb mecanismes de protecció elèctric.					

Taula 50-millora mecanismes de protecció elèctrica

Nom	**Monitorització dels sistemes d'informació.**					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-07	0	1/8/2017	2 mesos	Responsable de seguretat. Responsable de Sistemes d'informació	Comitè de seguretat	15.000 €
Objectius	• Conèixer l'estat en temps real del sistemes d'informació. • Poder detectar el mes aviat possible una interrupció del servei o un estat anòmal en els sistemes d'informació. • Establir mecanismes per protegir els registres obtinguts de la monitorització dels sistemes. • Sincronitzar rellotges.					
Descripció	Adquisició i posada en funcionament d'una plataforma de monitorització dels sistemes d'informació i implantació dels mecanismes necessaris per a generar alertes sobre el funcionament dels sistemes. La plataforma ha de ser capaç de monitoritzar l'estat del elements hardware i software dels sistemes i generar alertes en cas de mal funcionament o funcionalment anòmal. A més, la plataforma ha d'implementar mecanismes de gestió i protecció de registres obtinguts, mecanismes per garantir la cadena de custòdia y un servidor de temps per mantenir sincronitzats els rellotges de l'organització.					
Indicadors	• Percentatge de sistemes monitoritzats.					

Taula 51-millora monitorització

Nom	Redundància de la connexió de dades.					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-08	0	1/1/2017	2 anys	Responsable de seguretat. Responsable de Sistemes d'informació	Comitè de seguretat	30.000 €
Objectius	• Contractar una segona connexió a Internet.					
Descripció	L'accés a les aplicacions de negoci per part dels clients depèn en gran mesura de l'accés a Internet. Es important doncs garantir que les aplicacions poden seguir publicant-se a Internet en cas de caiguda de l'enllaç principal.					
Indicadors	• Número de vegades que s'ha encaminat la informació de dades a través de l'enllaç secundari.					

Taula 52-millora redundància connexió de dades

Nom	Adquisició d'una solució HA per als virtualitzadors.					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-09	0	1/7/2018	1 mes	Responsable de seguretat. Responsable de Sistemes d'informació	Comitè de seguretat	80.000 €
Objectius	• Aconseguir alta disponibilitat en els sistemes de virtualització.					
Descripció	Adquirir i configurar el hardware i software necessari per implementar una solució d'alta disponibilitat dels virtualitzadors. D'aquesta forma en cas de caiguda del virtualitzador actual es podrà garantir l'execució de les màquines virtuals en un altre node.					
Indicadors	• Número de vegades que una màquina s'ha mogut d'un virtualitzador a un altre.					

Taula 53-millora HA per virtualitzadors

Nom	**Millorar de la capacitació tècnica del personal de sistemes.**					
CODI	**Revisió**	**Inici**	**Durada**	**Responsable**	**Aprovació**	**Pressupost**
SI-PM-010	0	1/1/2017	2 anys	Responsable de seguretat. Responsable de Sistemes d'informació Responsable de RRHH	Comitè de seguretat	30.000 €
Objectius	• Reduir les incidències relacionades amb la no disponibilitat dels sistemes motivades per errors de configuració.					
Descripció	Identificar les accions formatives necessàries i punts de millora a fi i efecte d'implementar un conjunt d'iniciatives formatives als administradors dels sistemes. La iniciativa persegueix dotar als administradors de més coneixements sobre el seu entorn, reduir el temps que necessiten els administradors per resoldre incidències en els sistemes i reduir el nombre d'incidències derivades d'una incorrecta o error en la configuració.					
Indicadors	• Número d'accions formatives. • Percentatge d'incidències relacionades amb errors de configuració.					

Taula 54-millora capacitació tècnica

10.13. Annex evolució del risc

CLASSE	ID	VALOR	F	RISC					NOU RISC				
				C	I	D	A	T	C	I	D	A	T
[L]	L1	MA	FM	4,5	9	10	0	0	4,5	9	10	0	0
	L2	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L3	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L4	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L5	A	FA	2	90	70	0	0	0,2	9	7	0	0
	L6	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	L7	A	FA	10	16	100	0	0	1	1,6	10	0	0
[HW]	HW1	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	HW2	MA	FM	1,8	1,8	10	0	0	1,8	1,8	10	0	0
	HW3	A	FB	0,1	0,16	0,8	0	0	0,1	0,16	0,8	0	0
	HW4	A	FB	0,1	0,14	1	0	0	0,1	0,14	1	0	0
	HW5	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW6	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW7	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW8	A	FM	1,6	1,4	10	0	0	1,6	1,4	10	0	0
	HW9	MA	FM	1	1,4	10	0	0	1	1,4	10	0	0
	HW10	A	FB	0,1	0,14	1	0	0	0,1	0,14	1	0	0
[SW]	SW1	MA	FA	18	45	10	90	0	1,8	4,5	1	9	0
	SW2	B	FA	10	25	70	50	10	1	2,5	7	5	1
	SW3	MA	FA	18	45	100	90	18	1,8	4,5	10	9	1,8
	SW4	M	FA	16	45	60	100	16	1,6	4,5	6	10	1,6
	SW5	MA	FA	10	45	100	90	10	1	4,5	10	9	1
	SW6	B	FA	20	50	70	100	20	2	5	7	10	2
	SW7	MA	FA	20	40	100	100	20	2	4	10	10	2
	SW8	MA	FA	10	35	100	90	10	1	3,5	10	9	1
	SW9	A	FA	10	45	70	90	10	1	4,5	7	9	1
	SW10	MA	FA	10	45	100	90	10	1	4,5	10	9	1
	SW11	MA	FA	10	45	70	90	10	1	4,5	7	9	1
	SW12	B	FA	10	35	70	50	10	1	3,5	7	5	1
	SW13	A	FA	10	35	100	70	10	1	3,5	10	7	1
	SW14	A	FA	10	35	100	100	10	1	3,5	10	10	1
[D]	D1	MA	FB	0,5	0,9	1	0,9	0,5	0,5	0,9	1	0,9	0,5
	D2	A	FB	0,5	0,9	0,7	0,9	0,5	0,5	0,9	0,7	0,9	0,5
	D3	B	FB	1	1	0,7	1	1	1	1	0,7	1	1
	D4	MA	FB	1	1	0,5	1	1	1	1	0,5	1	1
	D5	MA	FB	1	1	0,5	1	1	1	1	0,5	1	1
	D6	M	FB	0,8	0,9	0,6	1	0,8	0,8	0,9	0,6	1	0,8
	D7	MA	FB	1	0,8	1	1	1	1	0,8	1	1	1

	D8	MA	FB	0,5	0,7	1	0,9	0,5	0,5	0,7	1	0,9	0,5
[COM]	COM1	A	FB	0,5	0,9	1	0,9	0	0,5	0,9	1	0,9	0
	COM2	MA	FB	0,5	0,7	1	0,9	0	0,5	0,7	1	0,9	0
[AUX]	AUX1	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX2	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX3	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX4	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX5	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX6	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX7	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX8	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX9	MA	FB	0	0	1	0	0	0	0	1	0	0
	AUX10	M	FB	0	0	1	0	0	0	0	1	0	0
	AUX11	A	FB	0	0	1	0	0	0	0	1	0	0
	AUX12	MA	FB	0	0	1	0	0	0	0	1	0	0
[P]	P1	MA	FM	0	0	1	0	0	0	0	1	0	0
	P2	MA	FM	0	0	1	0	0	0	0	1	0	0

Taula 55-evolució del risc

10.14. Auditoria interna d'acompliment

INFORMACIÓ DEL DOCUMENT	
Nom del document	APZ-2000 Auditoria interna d'acompliment

CONTROL DOCUMENTAL	
Autor: David González Mas	
	Aprovat per:
Nom	
Data	

REGISTRE DE REVISIONS		
Versió	**Data**	**Resum i motius de modificació**
1.0	1-9-2018	

Dades de l'auditoria

a) Dades de l'empresa

Raó Social	Autoritat Portuària de Zapata
CIF	CIF: Q4567890R
Adreça	Plaça de l'APZ s/n, Zapata
Contacte	info@apz.cat
Persona a càrrec	David González

Taula 56-dades de l'empresa a auditar

b) Dades de l'equip auditor

Auditor en Cap	RP
Auditor	AF

Taula 57-dades dels auditors

c) Pla d'auditoria

L'auditoria es realitzarà durant el mes de setembre de 2018. Un cop realitzada l'auditoria interna es procedirà al tractament de les no conformitats i la creació d'un mapa de ruta per executar els projectes necessaris per a solucionar-les.

Ubicació	Edifici d'oficines de l'APZ
Data d'inici	1 de Setembre de 2018
Duració	1 mes
Tipus d'auditoria	Interna

Taula 58-pla d'auditoria

Durant el procés d'auditoria es procedirà a entrevistar a tots els responsables i usuaris del SGSI, a la revisió dels controls tècnics i a la recol·lecció d'evidències per verificar l'acompliment de la norma.

d) Abast de l'auditoria

Avaluació del grau de compliment de la norma ISO 27001:2013 en el sistemes que donen suport a negoci:

- PCS
- Integra II
- Control d'accessos
- Sistema de telefonia

e) Aspectes de l'auditoria

Criteris de l'auditoria	• Marc de control ISO 27002:2013 • Anàlisi de riscos • Documentació SGSI • Criteri d'aplicabilitat
Documentació aplicable	• Sistema de certificació de l'APZ • Norma ISO/IEC 27001:2013 • Legislació aplicable a l'APZ
Objectiu de l'auditoria	
• Avaluació inicial de l'eficàcia del sistema de gestió en la seva totalitat, l'acompliment dels objectius de l'organització i la conformitat del sistema respecte als requeriments de les normes de referencia. • Obtenir evidències suficients i apropiades.	

Taula 59-aspectes de l'auditoria

f) Personal auditat

- Responsable de seguretat.
- Responsable de RRHH.
- Responsable d'instal·lacions.
- Responsable de Sistemes d'Informació.

Procés d'avaluació

Es valorarà la maduresa de la implantació del SGSI basant-se en el model CMM. Per afirmar que un SGSI està correctament implantat ha d'assolir, com a mínim, en nivell L3 (90%) en cadascun dels dominis que especifica la norma. Per a una millor visualització, es mostrarà una taula comparativa entre l'estat dels dominis inicial i el resultant després d'executar els projectes de la fase anterior:

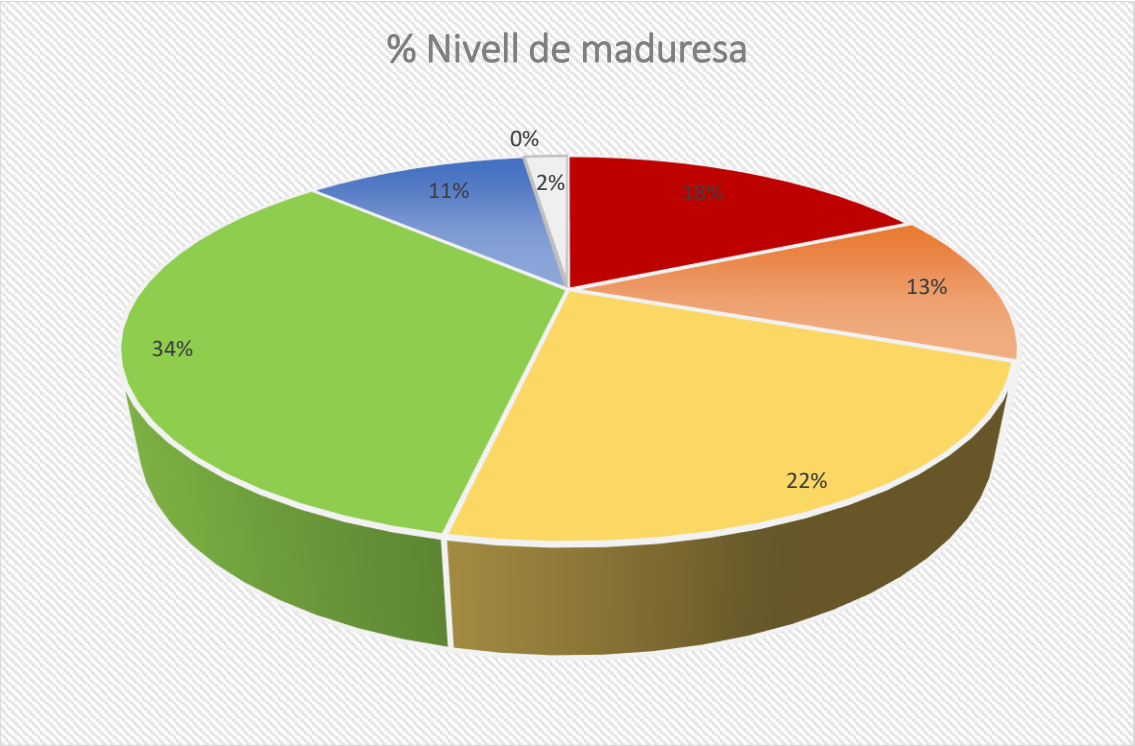
DOMINIS DE LA NORMA ISO 27002:2013	VALORACIÓ CMM	
	INICIAL	ACTUAL
[A.5] Política de seguretat	10%	90%
[A.6] Organització de la seguretat de la informació	18%	40%
[A.7] Gestió d'actius	66%	80%
[A.8] Seguretat dels recursos humans	67%	74%
[A.9] Seguretat física i ambiental	65%	65%
[A.10] Gestió de les comunicacions i operacions	56%	60%
[A.11] Control d'accessos	52%	70%
[A.12] Adquisició de sistemes d'informació, desenvolupament i manteniment.	12%	12%
[A.13] Gestió d'incidents de seguretat de la informació	16%	90%
[A.14] Gestió de la continuïtat de negoci	0%	90%
[A.15] Conformitat	56%	56%

Taula 60-auditoria evolució dominis

Llegenda CMM

ID	VALOR	ID	VALOR
L0	0%	L4	95%
L1	10%	L5	100%
L2	50%	L6	N/A
L3	90%		

Taula 61-llegenda CMM



Il·lustració 22-auditoria nivell de maduresa final

Pot observar-se que, una vegada implantats el projectes de millora proposats en l'apartat anterior, hi ha dominis que assoleixen el nivell L3. Per la resta es pot veure, que encara que no l'assoleixen, estan més a prop d'aconseguir-ho.

No conformitats

A continuació es mostra un resum de les no conformitats trobades durant el procés d'auditoria organitzades per domini.
Podem observar el detall de les no conformitats en les fitxes que es mostren a continuació.

DOMINI	NO CONFORMITATS	
	MAJORS	MENORS
[A.5] Política de seguretat		
[A.6] Organització de la seguretat de la informació	2	
[A.7] Gestió d'actius		1
[A.8] Seguretat dels recursos humans		1
[A.9] Seguretat física i ambiental		2
[A.10] Gestió de les comunicacions i operacions	1	1
[A.11] Control d'accessos		1
[A.12] Adquisició de sistemes d'informació, desenvolupament i manteniment.	1	
[A.13] Gestió d'incidents de seguretat de la informació		

[A.14] Gestió de la continuïtat de negoci		
[A.15] Conformitat		1

Il·lustració 23-no conformitat

AUDITOR	David González Mas	**DATA**	3 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Seguretat
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de seguretat
TIPUS DE NC	MAJOR		
DESCRIPCIÓ DE LA NC	• No s'evidencia l'existència de procediments que garanteixin el contacte amb autoritats rellevants. • No s'evidencia l'existència de procediments que garanteixin la revisió independent de la seguretat de la informació.		
REFERENCIA NORMATIVA	6.1.6, 6.1.8		
ACCIONS CORRECTIVES	1. Establir un procediment per garantir el contacte amb autoritats rellevants. 2. Establir un procediment per implicar el departament de seguretat de la informació en tot projecte de la Organització.	**DATA REVISIÓ**	2 de Gener de 2019
		RESPONSABLE	Responsable de seguretat

Taula 62-no conformitat 1

AUDITOR	David González Mas	**DATA**	3 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Seguretat
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de Seguretat
TIPUS DE NC	MAJOR		
DESCRIPCIÓ DE LA NC	• No s'evidencia l'existència de procediments per realitzar la gestió del risc associat a terceres parts i la gestió de la seguretat amb aquestes terceres parts, siguin clients o altres tipus de relacions.		
REFERENCIA NORMATIVA	6.2.1,6.2.2, 6.2.3		
ACCIONS CORRECTIVES	1. Establir un marc de referencia per	**DATA REVISIÓ**	2 de Gener de 2019

	garantir la gestió del risc i la seguretat amb terceres parts.	**RESPONSABLE**	Responsable de seguretat

Taula 63-no conformitat 2

AUDITOR	David González Mas	**DATA**	4 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Seguretat
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de Seguretat
TIPUS DE NC	MENOR		
DESCRIPCIÓ DE LA NC	• Tot i que existeix un conjunt de bones pràctiques per l'etiquetatge i gestió de la informació el procediment no està formalitzat ni es mesurable.		
REFERENCIA NORMATIVA	7.2.2		
ACCIONS CORRECTIVES	1. Redactar el procediment d'etiquetatge i gestió de la informació.	**DATA REVISIÓ**	2 de Gener de 2019
		RESPONSABLE	Responsable de seguretat

AUDITOR	David González Mas	**DATA**	5 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Recursos humans
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de recursos humans
TIPUS DE NC	MAJOR		
DESCRIPCIÓ DE LA NC	• Els nous contractes que es signen inclouen els termes i condicions del contracte, així com la responsabilitat del contractat en quan a termes de seguretat i classificació de la informació es refereix. Els contractes anteriors al 2015 no compleixen aquest requeriment.		
REFERENCIA NORMATIVA	8.1.3		
ACCIONS CORRECTIVES	1. Elaborar un procediment per actualitzar la informació de seguretat en els contractes vigents existents. 2. Generar un indicador per mesurar l'eficiència del procés.	**DATA REVISIÓ**	9 de Gener de 2019
		RESPONSABLE	Responsable de recursos humans

AUDITOR	David González Mas	**DATA**	6 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Instal·lacions
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable d'instal·lacions
TIPUS DE NC	MENOR		
DESCRIPCIÓ DE LA NC	• Tot i que existeix un conjunt de bones pràctiques no existeix un procés o conjunt de processos per evitar l'accés físic no autoritzat a les instal·lacions que gestionen informació de la organització.		
REFERENCIA NORMATIVA	9.1		
ACCIONS CORRECTIVES	1. Elaborar un procediment que garanteixi la implementació de mesures per evitar l'accés físic no autoritzat. 2. Generar un indicador per mesurar l'eficiència del procés.	**DATA REVISIÓ**	11 de Gener de 2019
		RESPONSABLE	Responsable d'instal·lacions

Taula 66-no conformitat 6

AUDITOR	David González Mas	**DATA**	6 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Instal·lacions
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable d'instal·lacions
TIPUS DE NC	MENOR		
DESCRIPCIÓ DE LA NC	• Tot i que existeix un conjunt de bones pràctiques no existeix un procés o conjunt de processos per garantir la protecció dels sistemes enfront les amenaces ambientals..		
REFERENCIA NORMATIVA	9.2		
ACCIONS CORRECTIVES	3. Elaborar un procediment que garanteixi l'establiment de mesures per garantir la protecció dels sistemes enfront les amenaces ambientals.	**DATA REVISIÓ**	11 de Gener de 2019
		RESPONSABLE	Responsable d'instal·lacions

	4. Generar un indicador per mesurar l'eficiència del procés.		

Taula 68-no conformitat 8 *Taula 67-no conformitat 7* **AUDITOR**	David González Mas	**DATA**	12 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Sistemes d'Informació
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de sistemes d'informació
TIPUS DE NC	MENOR		
DESCRIPCIÓ DE LA NC	• Tot i que existeix un conjunt de bones pràctiques i costums relacionades amb l'establiment de responsabilitats en l'operació, gestió dels servei entregat per terceres parts i protecció contra codi maliciós i mòbil no hi ha un procés definit.		
REFERENCIA NORMATIVA	10.1, 10.2, 10.4		
ACCIONS CORRECTIVES	1. Documentar els procediments i responsabilitats en l'operació. 2. Establir indicadors per mesurar l'entrega del servei prestat per terceres parts. 3. Establir mecanismes de control per evitar l'execució de codi mòbil.	**DATA REVISIÓ** **RESPONSABLE**	11 de Gener de 2019 Responsable de sistemes d'informació

<table>
<tr><td>AUDITOR</td><td>David González Mas</td><td>DATA</td><td>12 de Setembre de 2018</td></tr>
<tr><td>NORMATIVA</td><td>ISO 27001:2013</td><td>DEPARTAMENT</td><td>Sistemes d’Informació</td></tr>
<tr><td>TIPUS D’AUDITORIA</td><td>Interna d’acompliment</td><td>PERSONA AUDITADA</td><td>Responsable de sistemes d’informació</td></tr>
<tr><td>TIPUS DE NC</td><td colspan="3">MAJOR</td></tr>
<tr><td>DESCRIPCIÓ DE LA NC</td><td colspan="3">• No hi ha evidència de la existència de procediments ni mecanismes que garanteixin la correcta manipulació i gestió i destrucció de mitjans d’informació.
• No hi ha evidència de la existència de procediments, polítiques, acords per establir mecanismes d’intercanvi d’informació de manera correcta i segura.</td></tr>
<tr><td>REFERENCIA NORMATIVA</td><td colspan="3">10.7, 10.8</td></tr>
<tr><td rowspan="2">ACCIONS CORRECTIVES</td><td rowspan="2">1. Elaborar un procediment per establir mecanismes de manipulació, gestió i destrucció de mitjans d’informació.
2. Establir indicadors per mesurar l’eficiència del procediment.
3. Elaborar conjunt de polítiques per establir els mecanismes i controls per l’intercanvi d’informació així com la gestió i manipulació dels mitjans físics en trànsit.</td><td>DATA REVISIÓ</td><td>11 de Gener de 2019</td></tr>
<tr><td>RESPONSABLE</td><td>Responsable de sistemes d’informació</td></tr>
</table>

Taula 69-no conformitat 9

AUDITOR	David González Mas	**DATA**	18 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Sistemes d'Informació
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de sistemes d'informació
TIPUS DE NC	MAJOR		
DESCRIPCIÓ DE LA NC	• El procediment de revisió de permisos d'usuari no està formalitzat. • Els mecanismes de control per limitar el temps de connexió a la xarxa no estan formalitzats		
REFERENCIA NORMATIVA	11.2,11.5		
ACCIONS CORRECTIVES	4. Formalitzar el procediment de revisió de permisos d'usuari. 5. Formalitzar el conjunt de mecanismes per limitar el tempos de connexió a la xarxa i revisar la seva implementació en els sistemes.	**DATA REVISIÓ** **RESPONSABLE**	15 de Gener de 2019 Responsable de sistemes d'informació

Taula 70-no conformitat 10

AUDITOR	David González Mas	**DATA**	20 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Sistemes d'Informació
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de sistemes d'informació
TIPUS DE NC	MAJOR		
DESCRIPCIÓ DE LA NC	• Els requeriments de seguretat de les aplicacions no estan incorporats en la presa de requeriments en el desenvolupament de programari. • No hi ha cap tipus de procediment ni control per garantir el correcte processament d'informació per part de les aplicacions. • No existeix una política d'ús de controls criptogràfics ni un repositori controlat de claus.		

	• No s'incorpora la seguretat dins del procés de desenvolupament i suport a les aplicacions. • Noi existeix cap tipus de procediment ni control per avaluar i corregir les vulnerabilitats tècniques que pugui presentar un programa.		
REFERENCIA NORMATIVA	12.1, 12.2,12.3,12.4,12.5		
ACCIONS CORRECTIVES	• Incorporar la seguretat com un procediment transversal en el desenvolupament de codi, tant en les activitats d'anàlisi com desenvolupament i suport, incloent bones pràctiques de desenvolupament i controls per garantir el correcte processament de la informació. • Establir una política d'us de controls i certificats criptogràfics. Establir un repositori que permeti gestionar correctament els controls criptogràfics dels diferents usuaris.	**DATA REVISIÓ**	17 de Gener de 2019
		RESPONSABLE	Responsable de sistemes d'informació

Taula 71-no conformitat 11

AUDITOR	David González Mas	**DATA**	25 de Setembre de 2018
NORMATIVA	ISO 27001:2013	**DEPARTAMENT**	Sistemes d'Informació
TIPUS D'AUDITORIA	Interna d'acompliment	**PERSONA AUDITADA**	Responsable de sistemes d'informació
TIPUS DE NC	MENOR		
DESCRIPCIÓ DE LA NC	• Els procediment d'auditoria de seguretat no es planifiquen tenint en compte les necessitats de servei i operació de la resta de departaments.		
REFERENCIA NORMATIVA	15.2,15.3		

ACCIONS CORRECTIVES	• Realitzar un calendari d'auditories tenint en compte els requeriments d'operació de la resta de departaments.	**DATA REVISIÓ**	20 de Gener de 2019
		RESPONSABLE	Responsable de sistemes d'informació

Taula 72-no conformitat 12