Pla Director de Seguretat

Ajuntament de Fita Alta

Juny 2016

Nom Estudiant: Andreu Retamero Pallarès

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

Nom Consultor: Arsenio Tortajada Gallego
Professor responsable de l'assignatura: Carles Garrigues Olivella
Centre: Universitat Oberta de Catalunya

Data Lliurament: 06/06/2016

FITXA DEL TREBALL FINAL

Títol del treball:	***Implantació d'un Sistema de gestió de la seguretat de la informació en el Ajuntament de Fita Alta***
Nom de l'autor:	***Andreu Retamero Pallarès***
Nom del consultor:	***Arsenio Tortajada Gallego***
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*06/2016*
Titulació o programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea del Treball Final:	***Sistemes gestió seguretat informació***
Idioma del treball:	*Català*
Paraules clau	*ISO/IEC, 27002, 27001, ENS*

Resum del Treball (màxim 250 paraules):

El Treball de Fi de Màster consisteix en la realització d'un **Pla Director** per a un Ajuntament que li permeti gestionar de forma adequada la seguretat basada en les "bones pràctiques" en la gestió de la seguretat de la informació de la ISO/IEC 27002 i en les especificacions per a la implantació d'un sistema de gestió de la seguretat de la informació recollides en la ISO/IEC 27001.

Al ser un Ajuntament una administració pública, el Pla Director també ha d'ajustar-se a la normes jurídiques estatals, autonòmiques i locals que regulen l'ús de les TIC. En particular

- Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, i els seus dos reglaments de desenvolupament:

- Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat.

- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.

Abstract (in English, 250 words or less):

The Final Master is conducting a Master Plan for City Council to allow him to manage appropriately based security "best practices" in the management of information security ISO / IEC 27002 and the specifications for the implementation of a safety management system of information contained in the ISO / IEC 27001.

Being a City public administration, the Plan must also conform to the legal standards national, regional and local govern the use of ICT. in particular

- Law 11/2007 of 22 June, electronic access to public services, and their two implementing regulations:

- Royal Decree 3/2010 of 8 January, which approves the National Security Framework.

- Royal Decree 4/2010 of 8 January, which approves the National Interoperability Framework.

Paraules clau (entre 4 i 8):

ISO/IEC, 27002, 27001, ENS

Índex

1. Introducció

1.1. Context i justificació del Treball

Qualsevol administració pública, i en particular els ajuntaments, depenen de les Tecnologies de la Informació i les Comunicacions (TIC en endavant) per a poder oferir els serveis que li són propis a la ciutadania. Els seus sistemes TIC han de ser administrats amb diligència i s'han de prendre les mesures necessàries per a protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat, confidencialitat i autenticitat de la informació i dels serveis prestats així com garantir una traçabilitat de les operacions que es realitzen.

Els sistemes TIC han d'estar protegits contra amenaces que poden incidir en la confidencialitat, la integritat, la disponibilitat i l'autenticitat de la informació i dels serveis. Per a defensar-se d'aquestes amenaces cal desenvolupar eines que s'adaptin al canvis de l'entorn per a garantir la prestació continuada dels serveis.

El Reial decret 3/2010 pel qual s'aprova l'Esquema Nacional de Seguretat (en endavant ENS) i el Reial decret 951/2015 que el modifica especifiquen les mesures mínimes de seguretat exigides que han de seguir les administracions públiques en l'àmbit de l'administració electrònica. Aquestes normes garanteixen les bases que han de facilitar la continuïtat dels serveis prestats.

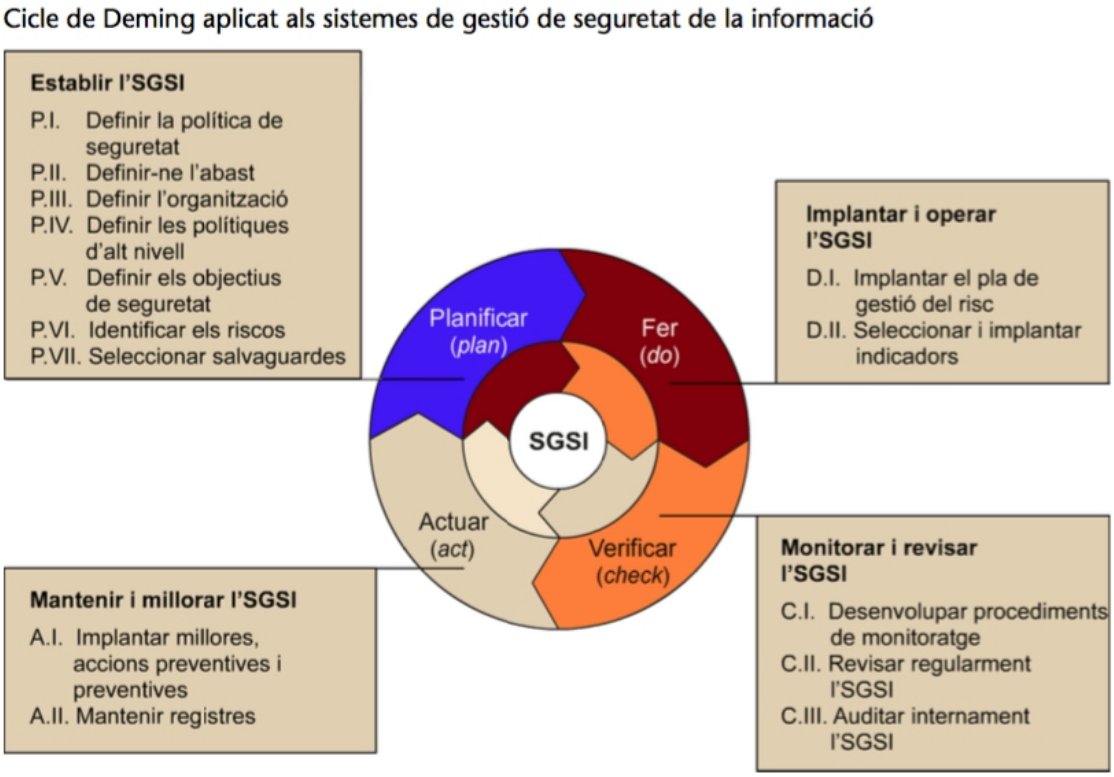
Una aproximació a la implantació de la seguretat en una administració pública podria ser centrar-se exclusivament en l'aplicació de les normes que se li apliquen i en particular de l'ENS. Les normes i recomanacions que regulen l'ENS recomanen veure la seguretat com un procés que formi part del cicle de vida dels sistemes TIC. La seva aplicació és basa en la realització d'una anàlisis de riscos i en l'aplicació de les seves salvaguardes articulades en un conjunt de projectes que l'adeqüin als nivells exigibles per la normativa vigent.

També es pot fer una aproximació més àmplia a la seguretat dels sistemes TIC fent la implantació d'un Sistema de Gestió de la Seguretat de la Informació (en endavant SGSI). Aquest enfoc incorpora dintre seu el descrit anteriorment per l'ENS però va més enllà ja que un SGSI segons la ISO 27001 "És un sistema de gestió que comprèn la política, l'estructura organitzativa, els procediments, els processos i els recursos necessaris per a implantar la gestió de la seguretat de la informació. ..... Aquest sistema proporciona mecanismes per al control de la seguretat dels actius de la informació i dels sistemes que els processen, en concordança amb les polítiques de seguretat i els plans estratègics de l'organització"

És en aquest context que la implantació d'un SGSI a l'Ajuntament és considera una forma efectiva i eficient d'assolir els requisits legals i alhora de garantir que les polítiques de seguretat estan alineades amb els plans estratègics i de negoci de l'organització en un sistema de millora contínua.

1.2. Objectius del Treball

La realització d'un Pla Director de Seguretat de la Informació que estableixi la fulla de ruta que ha de seguir l'Ajuntament de "Fita Alta" per a gestionar de forma adequada la Seguretat, permetent, no només conèixer l'estat d'aquesta, sinó també les línies on s'ha d'actuar per a millorar-la dintre d'un model de millora contínua PDCA (Plan-Do-Check-Act) que defineix la norma ISO/IEC 27001



La implantació d'unSGSI basat en la millora continua permetrà a l'Ajuntament de Fita Alta tractar la seguretat dels seus sistemes com un procés i anar-lo revisant periòdicament per a adaptar-lo a les noves necessitats legals, a la utilització de noves tecnologies, a l'aparició de noves amenaces de forma que se'n minimitzin els riscos.

Els principals objectius de la realització del Pla Director de la Seguretat de la Informació són:

- ✔ Compliment de la normativa legal en matèria de seguretat: ENS, LOPD
- ✔ Implantació de les bones pràctiques en Seguretat dels SGSI de les normes ISO/IEC 27000 (27001 norma certificable i 27002 recull de bones pràctiques)
- ✔ Millorar la seguretat dels sistemes de gestió de la informació de l'Ajuntament
- ✔ Oferir serveis segurs a la ciutadania
- ✔ Millorar la confiança que tenen els ciutadans en l'administració

1.3. Enfocament i mètode seguit

La metodologia seguida per a la realització del Pla Director ha estat seguir una aproximació per fases al projecte.

S'ha contemplat la realització de 6 fases:

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

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

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

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

- **Fase 3 : Anàlisi de riscos**

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

- **Fase 4 : Proposta de projectes**

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

- **Fase 5 : Auditoria de Compliment de la ISO/IEC 2702:2013**

  Avaluació de controls, maduresa i nivell de compliment.

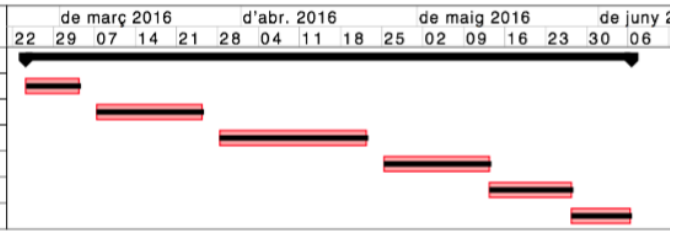
- **Fase 6 : Presentació de resultats i lliurament d'informes**

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

1.4. Planificació del Treball

La planificació de les diferents fases es pot veure al diagrama de GANTT del projecte i el detall dels resultats per a cada fase.

	Name	Start	Finish
1	**Treball Fi de Màster**	**24/02/16 08:00**	**06/06/16 17:00**
2	Situació actual : Cont..	24/02/16 08:00	04/03/16 17:00
3	Sistema de Gestió D...	07/03/16 08:00	25/03/16 17:00
4	Anàlisi de riscos	28/03/16 08:00	22/04/16 17:00
5	Proposta de projectes	25/04/16 08:00	13/05/16 17:00
6	Auditoria de Compli...	13/05/16 08:00	27/05/16 17:00
7	Presentació de resu...	27/05/16 08:00	06/06/16 17:00



Cada fase recull a l'apartat de tasques les fites parcials més importants a realitzar.

Fase 1	**Situació actual : Contextualització, objectius i anàlisi diferencial**		
Descripció	Introducció al Projecte. Enfoc i selecció de l'empresa objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisis diferencial de l'empresa amb respecte a la ISO/IEC 27001+ISO/IEC 27002		
Tasques a realitzar	- Descripció detallada de l'organització - Abast del Pla Director de Seguretat - Anàlisi diferencial / Anàlisi de compliment inicial		
Data d'inici	24/02/2016	**Data de fi**	04/03/2016

Fase 2	**Sistema de Gestió Documental**		
Descripció	Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI		
Tasques a realitzar	- Política de Seguretat - Procediment d'auditories internes - Gestió d'indicadors - Procediment de revisió per la direcció - Gestió de rols i responsabilitats - Metodologia d'anàlisi de riscos - Declaració d'aplicabilitat		
Data d'inici	04/03/2016	**Data de fi**	25/03/2016

Fase 3	**Anàlisi de riscos**		
Descripció	Elaboració d'una metodologia d'anàlisis de riscos: Identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.		
Tasques a realitzar	- Anàlisi detallat dels actius rellevant a nivell de seguretat - Estudi de les amenaces del sistema d'informació i del seu impacte - Avaluació de l'impacte potencial de la materialització de les diferents amenaces a les quals estan exposades els actius		
Data d'inici	25/03/2016	**Data de fi**	22/04/2016

Fase 4	Proposta de projectes		
Descripció	Avaluació de projectes que ha de portar a terme la Organització per alinear-se amb els objectius plantejats al Pla Director. Quantificació econòmica i temporal d'aquests.		
Tasques a realitzar	- Proposta de projectes - Temporalització i valoració econòmica		
Data d'inici	22/04/2016	**Data de fi**	13/05/2016

Fase 5	Auditoria de Compliment de la ISO/IEC 2702:2013		
Descripció	Avaluació de controls, maduresa i nivell de compliment.		
Tasques a realitzar	- Informe complert d'auditoria - Detall de les No-conformitats		
Data d'inici	13/05/2016	**Data de fi**	27/05/2016

Fase 6	Presentació de resultats i lliurament d'informes		
Descripció	Consolidació dels resultats obtinguts durant el procés d'anàlisi. Realització dels informes i presentació executiva a Direcció. Lliurament del projecte final.		
Tasques a realitzar	- Resum executiu - Presentació de defensa del Treball de Fi de Màster - Vídeo de defensa del Treball de Fi de Màster - Memòria del projecte que inclogui les tasques de totes les fases realitzades		
Data d'inici	27/05/2016	**Data de fi**	06/06/2016

1.5. Breu sumari de productes obtinguts

El Treball de Fi de Màster (TFM) de Sistemes de Gestió de la Informació no té com a objectiu la producció d'un conjunt de productes o eines desenvolupades adhoc per a resoldre una funcionalitat concreta. El resultat de totes les tasques del TFM és la realització d'un Pla Director per a l'adaptació del Sistema de Seguretat dels Sistemes d'Informació d'una organització als requisits i especificacions en matèria de seguretat que recomana la norma ISO/IEC 27001:2013 (norma certificable) i seguir el conjunt de bones pràctiques de la norma ISO/IEC 27002:2013.

El resultat d'aquest TFM és un conjunt de documents que recullen la realització de les tasques que hem comentat. Els documents que s'han elaborat com a materialització de les tasques realitzades són:

- ✔ "**Pla Director**" o "**Memòria del Projecte**" que inclou els documents i la feina feta a les fases realitzades

- ✔ **Resum executiu**: una descripció breu del projecte, el seu enfoc i les principals conclusions obtingudes.

- ✔ **Presentació** de defensa del Treball de Fi de Màster

- ✔ **Vídeo** de defensa del Treball de Fi de Màster d'una durada aproximada de 20 minuts

1.6. Breu descripció dels altres capítols de la memòria

En la primera fase s'han definit les bases de tot el posterior desenvolupament del projecte i s''ha seleccionat l'empresa objecte d'estudi, en el nostre cas l'Ajuntament de Fita Alta. Un cop seleccionada l'empresa s'ha realitzat una anàlisi detallada d'aquesta i s'ha definit amb claredat l'abast del Pla Director de Seguretat. S'ha realitzat una anàlisi diferencial per a comprovar el grau de compliment inicial de la norma 27002:2013.

En aquesta fase també ens hem documentat sobre la normativa de gestió de riscos que desenvoluparem i la normativa de referència que utilitzarem pel desenvolupament del projecte, ISO/IEC 27001:2013

En la segona fase s'ha desenvolupat tot l'esquema documental necessari per a poder certificar el sistema i que ha de tenir tot SGSI. Els documents elaborats han estat la Política de Seguretat, el Procediment d'auditories internes, la gestió d'indicadors, el procediment de revisió per la direcció, la gestió de rols i responsabilitats, la metodologia d'anàlisi de riscos i la declaració d'aplicabilitat.

Es pot veure que en aquesta segona fase s'ha establert la metodologia a seguir en alguna de les fases posteriors com l'anàlisi de riscos i la l'auditoria.

En la tercera fase s'ha realitzat una anàlisi de riscos seguint la metodologia MAGERIT proposada pel Consell Superior d'Administració Electrònica. Aquesta anàlisi ens ha facilitat:

- la identificació i valoració dels actius essencials de l'organització
- la definició de les amenaces a les que estan exposats aquests actius
- L'avaluació de l'impacte potencial que suposaria la materialització de les amenaces a les que estan exposats els actius

Una característica d'aquesta fase és que s'ha utilitzat l'eina EAR-PILAR del CCN-CERT per a fer l'anàlisi de riscos. Aquesta eina segueix la Metodologia Magerit. Utilitza una base de dades d'amenaces amb les probabilitats de materialització de les amenaces la qual cosa permet un càlcul del valor de risc residual avaluant les salvaguardes aplicades al SGSI. L'eina també permet la generació de múltiples informes que s'han utilitzat com a font d'informació per a la realització del TFM.

La quarta fase ha consistit en la realització d'un conjunt de projectes agrupats en un Pla de millora amb un doble objectiu: la implantació d'un SGSI que segueixi la norma ISO/IEC 27001:2013 i reduir el risc que té el sistema i que hem avaluat a la fase anterior.

El Pla de Millora contempla una execució d'aquests projectes en dos semestres de forma que al finalitzar l'any s'hagin assolit els objectius de la fase objectiu. Aquest Pla està dissenyat per a que el nostre SGSI s'acosti en un any al compliment de la norma però no l'assoleixi totalment. Al finalitzar l'any s'ha de revisar l'anàlisi de riscos i elaborar una nova proposta de projectes que ens portarà al compliment de la norma en la seva totalitat.

En la cinquena fase s'ha avaluat la maduresa de la seguretat pel que fa als diferents dominis de control plantejats per la ISO/IEC 27002:2013. S'ha realitzat un "Informe d'auditoria" fent la suposició que s'han implementat els projectes definits a la fase anterior.

I per a finalitzar, la sisena fase ha consistit en la recopilació de tota la informació generada en les fases anteriors per a donar-li el format adequat per a la seva presentació. S'han generat els següents documents:

- Resum executiu
- Presentació de defensa del Treball de Fi de Màster
- Vídeo de defensa del Treball de Fi de Màster
- Memòria del projecte que inclogui les tasques de totes les fases realitzades

2. Contextualització de l'empresa

2.1. Descripció de l'organització

Fita Alta és ciutat de referència al seu territori d'influència i ha superat els 100.000 habitants els darrers anys. La disponibilitat de sòl industrial ha suscitat la implantació de noves empreses i de llocs de treball. L'aposta per la innovació es materialitza en la creació d'un Parc Tecnològic on ja hi ha les bases operatives d'empreses tecnològiques d'alt nivell.

L'agroindústria, el comerç i el turisme són els sectors estratègics pel seu pes en l'economia de la ciutat. La tradició de gran productor i de centre de distribució agroalimentària ha evolucionat cap al disseny, desenvolupant i producció d'aliments innovadors i amb propietats beneficioses per a la salut dels consumidors.

L'Ajuntament de Fita Alta té aproximadament 700 treballadors propis i uns altres 100 repartits en diferents Instituts Municipals. Disposa un parc de 700 ordinadors que estan repartits entre uns 40 edificis repartits per tot el terme municipal. Encara que el 80 % dels equipaments estan ubicats en 15 edificis.

Els seus sistemes TIC estan constituïts per 2 CPD sincronitzats i ubicats en dos edificis diferents. La xarxa de telecomunicacions que interconnecta tots els edificis és pròpia i està gestionada per tècnics municipals. El serveis de telefonia corporatiu utilitzen telefonia IP i està gestionat pels tècnics de TI propis de la corporació. Els servidors corporatius utilitzen la tecnologia de Virtualització i estan basats en sistemes operatius Linux en prop d'un 90%. Les bases de dades utilitzades són Oracle i amb menys mesura MySQL.

El departament de TI està compost per aproximadament 20 persones repartides en 4 departaments: Centre d'atenció a l'usuari (3), Informació de Base (5), Desenvolupament d'aplicacions (5), Infraestructura tecnològica (5) i Administració (2).

2.2. Abast del Pla Director de Seguretat

Els Sistemes d'Informació de l'Ajuntament estan dividits en diferents subdominis:

- **Seu Electrònica**
- Web municipal
- Transparència
- Centre de Procés de dades
- Intranet

L'abast del Pla Director de Seguretat es centra en els Sistemes d'Informació del subdomini "Seu Electrònica" que és el domini on l'Ajuntament de Fita Alta ofereix els seus serveis a la ciutadania i les empreses i és el canal de comunicació electrònica.

El "subdomini Seu Electrònica" correspon al lloc web on l'Ajuntament de Fita Alta té la seva seu electrònica la qual es pot consultar a https://seu.fitaalta.cat . La Seu electrònica" és un punt d'accés únic a disposició de la ciutadania i de les empreses que representa una nova manera de realitzar les gestions públiques, sense condicionaments horaris ni d'espai, amb la màxima seguretat i contribuint a un ús més eficaç i eficient dels recursos públics. Es configura una oficina virtual oberta a totes hores i tots els dies de l'any.

La Seu electrònica és el lloc accessible per mitjans electrònics a través d'Internet per donar compliment a la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics, des d'on els ciutadans poden exercir el seu dret d'accés a la informació, als serveis i als tràmits de l'administració pública de manera telemàtica. I així, també, se n'assegura la disponibilitat, l'accés, la integritat, l'autenticitat, la confidencialitat i la conservació de les dades que s'hi gestionen.

La seu electrònica de l'Ajuntament de Fita Alta ofereix a ciutadans i empreses els serveis electrònics i el catàleg dels tràmits que s'ofereixen.

El "catàleg de tràmits" ofereix informació de tots els tràmits que es poden realitzar a l'Ajuntament de Fita Alta tan si aquests són telemàtics com presencials. Els tràmits es poden consultar de forma alfabètica o bé per temàtiques (beques i ajuts, comerç i consum, Cultura, Educació, ...). Hi ha un cercador de tràmits per a facilitar la recerca.

Els "Serveis" accessibles des de la seu electrònica són:

- El Tauler electrònic d'Edictes
- Licitacions de l'Ajuntament i dels organismes autònoms
- Pagament de tributs
- Consulta d'ordenances i reglaments
- Consulta del planejament urbanístic
- Consulta de les notificacions electròniques
- Carpeta ciutadana
- Carpeta del proveïdor
- Validador de documents electrònics
- Presentació de factures electròniques
- Consulta de les cartes de servei a la ciutadania

A nivell legal el subdomini "Seu electrònica" està sota l'aplicació del Reial Decret 3/2010, de 8 de gener (BOE de 29 de gener), pel qual es regula l'Esquema Nacional de Seguretat ("ENS") en l'àmbit de l'administració electrònica, dóna resposta al que preveu l'article 42 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (en endavant "Llei 11/2007"). Aquest article reconeix que la necessària generalització de la Societat de la Informació requereix la generació de confiança en els ciutadans la relació a través de mitjans electrònics i es fixa com a objectiu el crear les condicions de confiança necessàries en l'ús d'aquests mitjans.

Així doncs, la finalitat principal de l'ENS és establir la política de seguretat en la utilització de mitjans electrònics per part de les Administracions Públiques sotmeses a l'àmbit d'aplicació de la Llei 11/2007. Està constituït per aquells principis bàsics i els requisits mínims que permetin una protecció adequada de la informació. Això implica que la normativa obligatòria a aplicar al subdomini "Seu electrònica" és l'ENS a diferència de la resta de dominis on no hi ha una obligació legal a fer-ho i per tant agafarem la ISO 27001 com a model normatiu de referència.

2.3. Anàlisi de Compliment Inicial

2.3.1. Model de Maduresa de la Capacitat (CMM)

Abans de començar amb el projecte d'implantació, hem de realitzar un anàlisis diferencial de les mesures de seguretat i la normativa que tingui la Organització en relació a la Seguretat de la Informació. Aquest anàlisis diferencial es realitzarà respecte a als 114 controls o mesures preventives , organitzats en 14 àrees o dominis i 35 objectius de control de la i ISO/IEC 27002, i ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

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

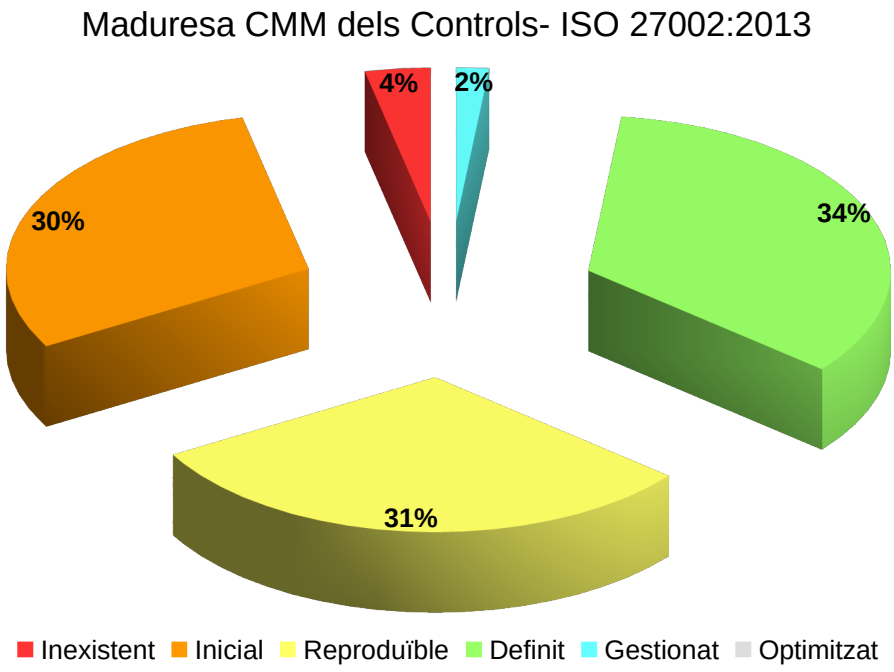
Efectivitat	CMM	Significat	Descripció
0%	L0	Inexistent	No hi ha una definició de responsabilitats en matèria de seguretat de la informació.
10%	L1	Inicial / Ad-hoc	Les responsabilitats principals s'assignen o assumeixen informalment. Cada persona sap la seva responsabilitat, però no la dels altres.
50%	L2	Repetible, però intuïtiu	Se sap qui assumeix les funcions principals en matèria de seguretat de les TIC i de la resta del negoci, però les funcions de seguretat no estan definides ni documentades específicament, sinó que s'assumeixen individualment com a part d'altres funcions (per exemple, la direcció d'un projecte).
90%	L3	Definit	Existeix, amb algunes deficiències. Les responsabilitats en seguretat de la informació s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, s'han donat a conèixer i s'ha fet o planificat la capacitació de totes les persones que ho requereixin.
95%	L4	Gestionat i mesurable	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, però no es fa una revisió anual per a verificar que totes les funcions s'han assignat bé i que els responsables desenvolupen la seva funció.
100%	L5	Optimitzat	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, es revisa periòdicament el desenvolupament d'aquestes funcions i hi ha un procés per a detectar deficiències en l'assignació i coordinació de funcions i per a aplicar-hi correccions.

Aquesta valoració ens servirà per a saber quin és l'estat actual de la seguretat a la nostra organització i per a saber quan allunyats estem dels objectius que volem assolir.

2.3.2. Presentació de resultats

Els resultats presentats en aquest punt corresponen a una primera estimació realitzada amb un full de càlcul per a tenir una primera aproximació al compliment inicial de la norma. Aquesta primera aproximació no serà tan acurada com la que es presenta en el punt "3 – Anàlisi diferencial" realitzat amb l'eina PILAR després d'una avaluació completa i detallada.

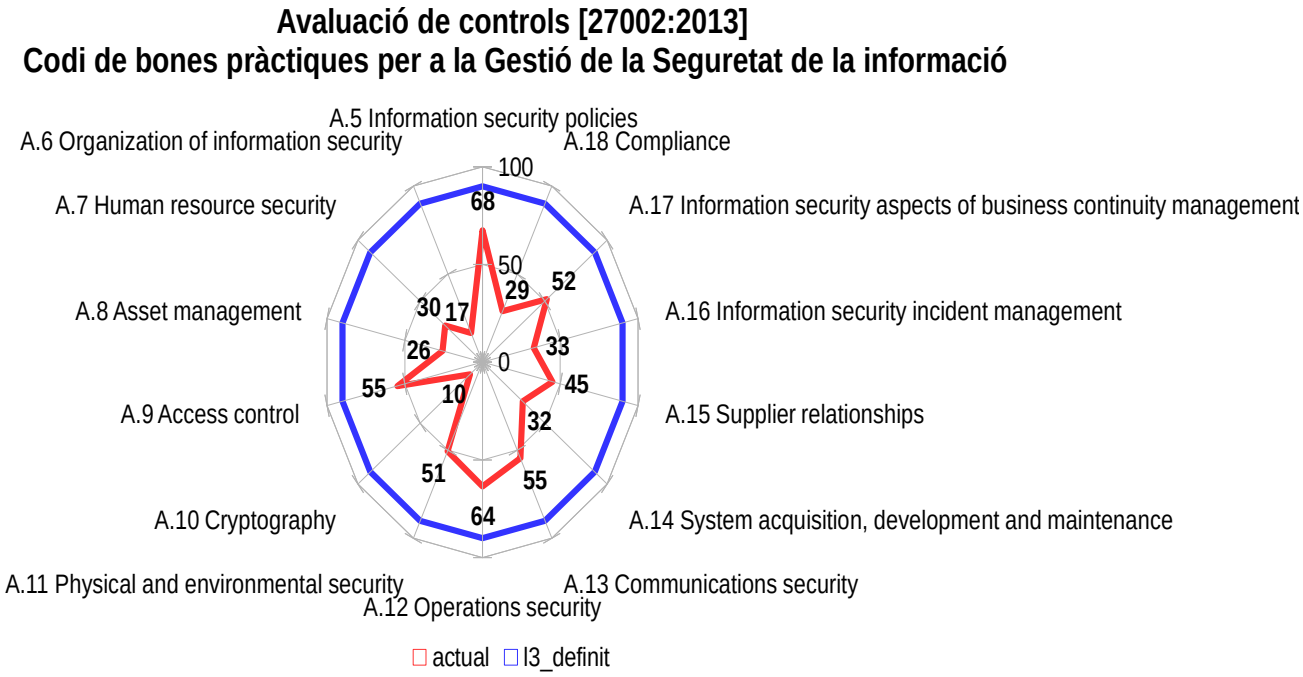
La gràfica percentual del nivell de maduresa dels 114 controls ens permet donar una visió de conjunt de l'estat de la seguretat.



És pot veure que el grup majoritari de Controls és L3-Definit amb 34,2% dels controls (efectivitat entre el 50% i el 90%). El segon grup és L2-Reproduïble amb el 30,7% dels controls (efectivitat entre el 10% i el 50%) seguit per L1 amb el 29,8% dels controls (efectivitat del 10%). La resta de nivells de maduresa són gairebé anecdòtics. Només n'hi ha el 3,5% dels que tenen una efectivitat inexistent corresponent al nivell L0 i el 1,75% que tenen una eficiència entre el 90% i el 95% que corresponen al nivell L4. Val a dir que no n'hi ha cap que correspongui al nivell L5 – Optimitzat amb un 100% d'efectivitat.

La visió de conjunt facilitada pel CMM indica que queda molt de camí per recórrer a l'organització per a arribar al nivell mínim de L3–Definit que correspondria a un nivell d'efectivitat entre el 50% i el 90% ja que el 64% dels controls no arriben a aquest nivell. I això sense tenir en compte que els que hem comptat com a nivell L4-Definit no vol dir que estiguin a un nivell del 90% d'efectivitat sinó que es mou en la forquilla que hi ha entre el 50% i el 90%.

Per a tenir una visió més detallada presentarem un "diagrama de radar" que mostra el compliment dels controls per a cada capítol o domini de la ISO. En aquest gràfic és on es veu de forma més clara la comparació entre l'estat actual i l'estat desitjat que correspondria a un nivell de compliment del 90% equivalent a L4-Procés definit.



En aquest diagrama es pot veure amb claredat que només hi ha dos capítols o dominis on la situació actual superi amb claredat el nivell **L2-Reproduïble** i que corresponen als dominis "*A.5 Information security policies*" i "*A.12 Operations security*" però que encara els hi falta molt per a arribar a nivells L3-Definit amb una efectivitat del 90% que és l'objectiu mínim a assolit.

Hi ha 4 dominis que si que assoleixen el nivell L2 completament però en canvi hi ha 7 dominis que no hi arriben clarament denotant així la diferència entre l'estat actual de compliment i el marcat per la norma.

2.3.3. Anàlisi diferencial

L'anàlisi diferencial està detallat a l'informe "Compliment de la norma" de l'eina µPILAR. Aquest informe presenta els resultats basant-se en el Model de Maduresa de la Capacitat (CMM) i es pot consultar a l'Annex IV – Compliment de la Norma 27002:2013 – Eina PILAR.

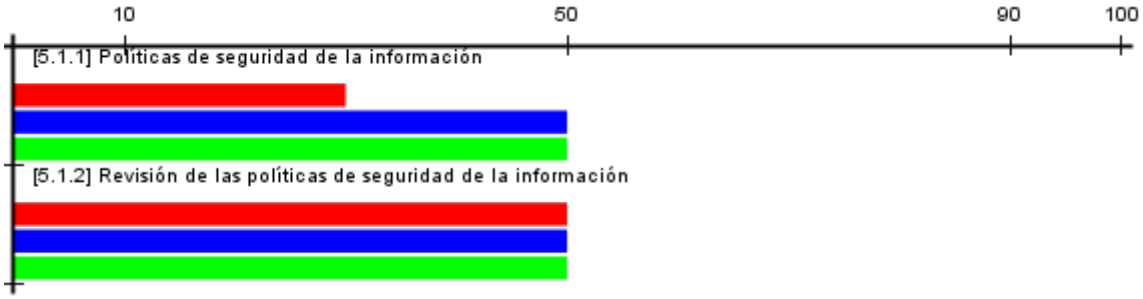
Es realitza respecte a als 114 controls o mesures preventives , organitzats en 14 àrees o dominis i 35 objectius de control de la i ISO/IEC 27002, i ens permet conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

L'informe de l'eina µPILAR no es limitat només a avaluar el compliment de la norma a l'estat "actual" sinó que també ho fa per a la fase intermèdia anomenada "Objectiu" i per a la fase final de l'estudi anomenada "PILAR". Aquesta triple valoració dels compliments és un dels valors afegits de fer l'anàlisi de riscos amb les eines PILAR.

La presentació de resultats de l'informe de l'eina PILAR variarà respecte als resultats presentats al punt 2 ja que aquests són fruit d'una avaluació manual feta amb un full de càlcul amb l'objectiu de fer una primera estimació. En canvi els resultats de PILAR corresponen a una avaluació molt més detallada i acurada.

Es mostra un exemple de l'anàlisi del compliment de la norma detallat a l'informe de Compliment de la Norma 27002:2013 de l'Eina PILAR per al domini de Polítiques de seguretat de la informació.

[5] Políticas de seguridad de la información



[actual] situación actual
[objetivo] situación objetivo
[PILAR] recomendación

[base] Base

control	[actual]	[objetivo]	[PILAR]
[5] Políticas de seguridad de la información	L1-L2	L2	L2
[5.1] Dirección de la gestión de la seguridad de la información	L1-L2	L2	L2
[5.1.1] Políticas de seguridad de la información	L1-L2	L2	L2
[5.1.2] Revisión de las políticas de seguridad de la información	L2	L2	L2

3. Esquema documental

Són els documents mínims necessaris per a poder certificar el sistema analitzat amb la norma ISO/IEC 27001.

3.1. Política de seguretat

Qualsevol administració pública, i en particular els ajuntaments, depèn de les Tecnologies de la Informació i les Comunicacions (TIC en endavant) per a poder oferir els serveis a la ciutadania que li són propis. Els seus sistemes TIC han de ser administrats amb diligència i s'han de prendre les mesures necessàries per a protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat, confidencialitat i autenticitat de la informació tractada i dels serveis prestats així com garantir una traçabilitat de les operacions que es realitzen.

L'article 11.1 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica (en endavant, l'ENS) estableix que tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent. Aquesta política de seguretat s'ha d'establir sobre la base dels principis bàsics indicats i s'ha de desenvolupar aplicant els requisits mínims següents:

a) Organització i implantació del procés de seguretat.
b) Anàlisi i gestió dels riscos.
c) Gestió de personal.
d) Professionalitat.
e) Autorització i control dels accessos.
f) Protecció de les instal·lacions.
g) Adquisició de productes.
h) Seguretat per defecte.
i) Integritat i actualització del sistema.
j) Protecció de la informació emmagatzemada i en trànsit.
k) Prevenció davant altres sistemes d'informació interconnectats.
l) Registre d'activitat.
m) Incidents de seguretat.
n) Continuïtat de l'activitat.
o) Millora contínua del procés de seguretat.

Així mateix, l'article 11.2 de l'ENS indica que, als efectes que indica l'apartat anterior, es consideren òrgans superiors els responsables directes de l'execució de l'acció del Govern, central, autonòmic o local, en un sector d'activitat específic, d'acord amb el que estableix la Llei 6/1997, de 14 d'abril, d'organització i funcionament de l'Administració General de l'Estat, i la Llei 50/1997, de 27 de novembre, del Govern; els estatuts d'autonomia corresponents i normes de desplegament; i la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, respectivament.

L'Ajuntament de Fita Alta ha decidit fer una aproximació més àmplia a la seguretat dels sistemes TIC implantant un Sistema de Gestió de la Seguretat

de la Informació (en endavant SGSI) basat en la norma ISO 27001:2013 adoptant les "bones pràctiques" i la metodologia sobre seguretat de la informació de la norma 27002:2013.

El compliment de les normes 27001 és complementari al descrit anteriorment per l'ENS. Un SGSI segons la ISO 27001 "És un sistema de gestió que comprèn la política, l'estructura organitzativa, els procediments, els processos i els recursos necessaris per a implantar la gestió de la seguretat de la informació. ..... Aquest sistema proporciona mecanismes per al control de la seguretat dels actius de la informació i dels sistemes que els processen, en concordança amb les polítiques de seguretat i els plans estratègics de l'organització"

És en aquest context que la implantació d'un SGSI a l'Ajuntament és considera una forma efectiva i eficient d'assolir els requisits legals i alhora de garantir que les polítiques de seguretat estan alineades amb els plans estratègics i de negoci de l'organització dintre d'un sistema de millora contínua.

3.1.1. Introducció

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces que poden incidir en la confidencialitat, integritat, disponibilitat i autenticitat de la informació i dels serveis. Per a defensar-se d'aquestes amenaces cal desenvolupar eines que s'adaptin al canvis de l'entorn per a garantir la prestació continuada dels serveis.

El Reial decret 3/2010 pel qual s'aprova l'Esquema Nacional de Seguretat (en endavant ENS) i el Reial decret 951/2015 que el modifica especifiquen les mesures mínimes de seguretat exigides que han de seguir les administracions públiques en l'àmbit de l'administració electrònica. Aquestes normes garanteixen les bases que han de facilitar la continuïtat dels serveis prestats.

L'Ajuntament de Fita Alta ha d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

L'Ajuntament de Fita Alta ha d'estar preparat per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'ENS.

3.1.1.1. Prevenció

L'Ajuntament de Fita Alta ha d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per això els departaments han d'implementar les mesures mínimes

de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política, els departaments han de:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.
- Demanar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

3.1.1.2. Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, els serveis s'han de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació i actuar en conseqüència segons el que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i informe que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com normals.

3.1.1.3. Resposta

L'Ajuntament de Fita Alta ha de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb el Centre de Seguretat de la Informació de Catalunya.

3.1.1.4. Recuperació

Per garantir la disponibilitat dels serveis crítics, l'Ajuntament de Fita Alta ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

3.1.2. Abast

Aquesta política s'aplica a tots els sistemes TIC de l'Ajuntament de Fita Alta i dels seus organismes autònoms sense excepcions. També és d'aplicació a terceres parts que gestionin serveis per compte de l'Ajuntament tal i com es recull en l'apartat 2.11 d'aquesta política de seguretat.

Això inclou el maquinari, el programari, la integració de sistemes i els serveis de consultoria d'acord amb la declaració d'aplicabilitat del SGSI.

3.1.3. Missió

L'Ajuntament de Fita Alta expressa el seu compromís amb l'administració de la seguretat de la seva informació, d'acord amb els requeriments propis, així com amb les lleis i normatives vigents.

L'Ajuntament de Fita Alta entén la seguretat com un principi per garantir el funcionament del servei públic i garantir els drets dels ciutadans i de la societat en general.

3.1.4. Marc normatiu

L'ús de les TIC per part de l'Ajuntament de Fita Alta es troba regulat per les següents normes jurídiques:

INTERNACIONAL

- ISO/IEC 27001:2013 – és la certificació que han d'obtenir les organitzacions. Norma que especifica els requisits per a la implantació del SGSI.
- ISO/IEC 27002:2013 codi de bones pràctiques per a la gestió de la seguretat de la informació. Prèviament BS 7799 Part 1 i la norma ISO/IEC 17799.

ESTATAL

- Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, i els seus dos reglaments de desenvolupament:
    - Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat.
    - Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Reial decret 1671/2009, de 6 de novembre, pel que es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Llei orgànica 15/1999, de 13 de desembre, de protecció de les dades de caràcter personal.
- Reial decret 1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reial decret 951/2015, de 23 d'octubre, de modificació del Real Decreto 3/2010, de 8 de gener, per qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.

AUTONÒMICA

- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya.

3.1.5. Dades de caràcter personal

L'Ajuntament de Fita Alta tracta dades de caràcter personal. El document de seguretat que es pot trobar a la Intranet defineix els components i els processos necessaris per complir amb la legislació vigent en l'àmbit de la seguretat del tractament de dades de caràcter personal. L'inventari de fitxers que es pot trobar a la intranet recull els fitxers afectats i els responsables corresponents.

Tots els sistemes d'informació de l'Ajuntament de Fita Alta s'han d'ajustar als nivells de seguretat requerits per la normativa per la naturalesa i finalitat de les dades de caràcter personal recollides en l'esmentat document de seguretat.

3.1.6. Gestió de riscos

Tots els sistemes subjectes a aquesta política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. Aquesta anàlisi es repetirà:

- Regularment, almenys un cop l'any.
- Quan canviï la informació manejada.
- Quan canviïn els serveis prestats.
- Quan es produeixi un incident greu de seguretat.
- Quan es reporten vulnerabilitats greus.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TIC establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats d'acord a les directrius dels responsables de la informació dels serveis. El Comitè de Seguretat TIC dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

3.1.7. Desenvolupament de la política de seguretat de la informació

Aquesta política s'ha de desenvolupar per mitjà de normativa de seguretat que afronti aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions. La normativa de seguretat estarà disponible a la intranet.

3.1.8. Obligacions del personal

Tots els membres de l'Ajuntament de Fita Alta tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de

Seguretat, i és responsabilitat del Comitè de Seguretat Corporativa disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'Ajuntament de Fita Alta atendran a una sessió de conscienciació en matèria de seguretat TIC que es repetirà periòdicament com a mínim un cop l'any supeditat a la disponibilitat pressupostària i de recursos. S'establirà un programa de conscienciació contínua per atendre tots els membres de l'Ajuntament de Fita Alta, en particular als de nova incorporació.

3.1.9. Terceres parts

Quan l'Ajuntament de Fita Alta presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per informació i coordinació dels respectius Comitès de Seguretat i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament de Fita Alta utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que pertoqui a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informació i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant en la prestació dels serveis.

3.2. Procediment d'Auditories Internes

La comprovació de la idoneïtat del disseny i la implantació del SGSI es fa amb auditories, que es poden fer internament o contractant auditors externs. Els auditors han de complir els següents requisits:

- Ser independents. No poden haver intervingut en el procés o treball auditat.
- Estar qualificats i, si pot ser, han de tenir experiència en el camp de la seguretat de la informació.

L'auditoria es pot plantejar com una activitat aïllada que es fa una única vegada, sovint quan es tracta d'auditories de segones o terceres parts per a obtenir una certificació o bé plantejar-la com un objectiu estratègic per a garantir la implantació i la millora del SGSI. En aquest segon plantejament les diferents auditories que es realitzen en el temps no es fan de manera independent les unes de les altres, sinó que són organitzades per a gestionar la funció d'auditoria en l'organització. És en aquest context que es crea el que s'anomena "Programa d'Auditoria", que no és més que un conjunt d'auditories planificades per a un període de temps i amb un objectiu d'auditoria comú, encara que cadascuna en tingui un de més específic.

L'Ajuntament de Fita Alta ha decidit implantar un "Programa d'Auditoria" per a garantir la idoneïtat i millora del seu SGSI, garantint així la preparació per a les futures auditories de renovació de la certificació del la ISO/IEC 27001:2013.

3.2.1. Programa d'auditoria

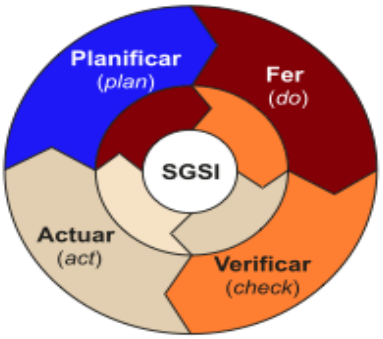
Un programa d'auditoria és més que tenir un conjunt d'auditories planificades en el temps. És la realització d'un pla de millora contínua basat en el cicle PDCA (**P**lan, **D**o , **C**heck, **A**ct) on el sistema que s'està implantant és la realització d'auditories pròpiament dita. Aquest pla s'implanta per aplicar la millora del SGSI utilitzant l'auditoria com l'eina o control de millora.

El programa d'auditoria és la realització d'un conjunt d'auditories separades amb el temps i amb objectius específics que col·laboren per a assolir un objectiu comú al de les auditories individuals.

Els programes d'auditoria ajuden al responsables de les funcions d'auditoria d'una empresa en la planificació de recursos i esforços necessaris per a realitzar les auditories i els seus resultats així com a millorar la capacitació del personal intern auditor.

La planificació de múltiples auditories per a assolir l'objectiu de monitorització i millora continuu del SGSI es realitza en organitzacions ja que tenen implantats sistemes de gestió estandarditzats i normalitzats on la tasca d'auditoria és un procés assumit per l'organització i es realitza, al menys, en part personal propi.

Un programa d'auditoria ha d'incloure com a mínim els 4 passos del cicle PDCA.



Cicle de Deming o cicle PDCA

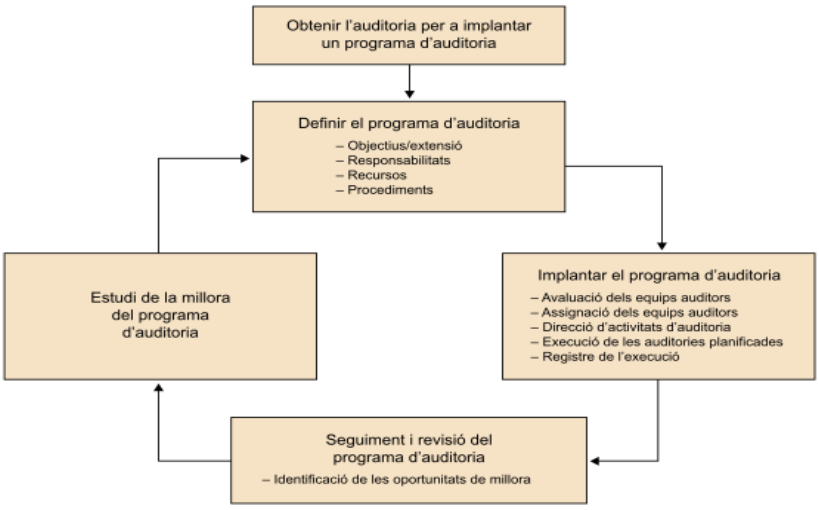


Diagrama general de la gestió d'un programa d'auditoria

Planificar o definir el programa d'auditoria

- Establir els objectius i extensió del programa d'auditoria
- Establir les persones responsables del programa d'auditoria
- Estimar i planificar els recursos necessaris

Do o Implantar el programa d'auditoria

Check o Seguiment i revisió del programa d'auditoria

Act o Estudi de la millora del programa d'auditoria

3.2.2. Assignació de rols

3.2.2.1. Persones, departaments i entitats

Les persones, departaments o entitats que participaran en el programa d'Auditoria de l'Ajuntament de Fita Alta són:

- Responsable de Seguretat

És la persona encarregada de supervisar la definició del programa d'auditoria i de presentar-lo al Comitè de Seguretat. Vetllarà per a que el programa d'auditoria tingui els recursos necessaris per al seu correcte funcionament i decidirà si, cal o no cal, suport extern i proposar la contractació d'una entitat externa per a que realitzi totes o alguna de les auditories planificades al Pla d'Auditoria.

Ha de decidir, i elevar al comitè de seguretat per a la seva aprovació, si cal que l'organització faci una inversió en eines de suport documentals per a la realització d'auditories com eines tècniques que ajudin a la recollida d'evidències i establiment de registres.

El responsable de seguretat, concretament, s'encarregarà de:

- Establir els objectius i l'extensió del programa d'auditoria
- Determinar les persones responsables
- Avaluació i assignació dels equips auditors
- Seguiment i supervisió del programa
- Estudi de la millora del programa d'auditoria.

- Comitè de Seguretat

Aprovarà el programa d'auditoria i li assignarà recursos per a que la seva implantació sigui possible.

Concretament s'encarregarà de:

- Aprovació del Pla d'auditoria
- Revisió anual del programa d'assessoria

- Servei de Tecnologies de la Informació i les Telecomunicacions

El personal de la gestió i manteniment dels sistemes d'informació i de les xarxes de telecomunicacions. Aquestes funcions fan que siguin susceptibles de poder participar en algunes auditories amb el rol de «expert tècnic» quan els seus coneixements o habilitats siguin requerits.

- Entitat/s externa/es d'auditoria

L'auditoria anual de compliment de la norma ISO/IEC 27001:2013 s'encarregarà a una entitat externa independent.

Aquesta entitat estarà acompanyada pel personal de l'Ajuntament de Fita Alta que els hi donaria suport en el procés d'auditoria. Aquest suport serviria, a més, per a que el personal intern adquireixi experiència i formació sobre la realització pràctica d'auditories internes.

Funcions de l'entitat externa auditora :

- Direcció de les activitats d'auditoria
- Execució de les auditories planificades
- Registre de l'execució de les auditories
- Elaboració de l'informe de l'auditoria.

3.2.2.2. Rols

Els rols del l'equip auditor i les persones, entitats o organitzacions que els realitzaran són els següents:

Responsable del programa d'auditoria → Responsable de seguretat

Auditor en cap (d'una auditoria particular) pot ser qualsevol dels dos següent:
→ Auditor d'una entitat externa (en el cas d'auditories externes de primera part o de tercera part en el cas de l'auditoria de certificació).
→ Responsable de seguretat (en el cas d'auditories internes de primera part)

Auditor (d'una auditoria particular) pot ser qualsevol dels dos següents:
→ Auditor d'una entitat externa (en el cas d'auditories externes de primera part o de tercera part en el cas de l'auditoria de certificació).
→ Responsable de seguretat.

Expert tècnic (d'una auditoria particular):
→ Personal del Servei de Tecnologies de la informació i les Telecomunicacions

3.2.3. Compromís de la direcció

El compromís de la direcció de l'Ajuntament de Fita Alta s'expressa ambla revisió anual que del Pla d'Auditoria que realitza el Comitè de Seguretat el qual dotarà dels recursos tècnics, econòmics de personal i de personal necessaris per a poder mantenir aquest Pla d'auditoria.

3.2.4. Planificació

La planificació és realitza dintre d'un Pla d'auditoria temporalitzat a 3 anys que és el període que cobreix la certificació del SGSI a la norma ISO/IEC 27001:2013.

El compliment de la norma ISO/IEC 27001:2013 suposa que el manteniment del SGSI ha de contemplar la revisió de 14 dominis, 35 objectius i 114 controls.

El Pla d'auditoria agrupa dominis amb característiques similars de forma que puguin ser revisats en una única auditoria parcial i es planifiquen aquestes amb l'objectiu d'assegurar el SGSI i de contribuir a la millora contínua de forma que, com a mínim, un cop a l'any siguin revisats tots els dominis, objectius i controls.

Els dominis contemplats a la noma ISO 27001:2013 són:

5	**Information security policies**.	(Política de Seguretat)	**1** Objectiu, **2** Controls
6	**Organization of information security**	(Organització de la seguretat de la informació)	**2** Objectius, **7** Controls
7	**Human resource security**	(Seguretat relativa al personal)	**3** Objectius, **6** Controls
8	**Asset management**	(Gestió d'actius)	**3** Objectius, **10** Controls
9	**Access control**	(Control d'accés)	**4** Objectius, **14** Controls
10	**Cryptography**	(Criptografia)	**1** Objectiu, **2** Controls
11	**Physical and environmental security**	(Seguretat física i de l'entorn)	**2** Objectius, **15** Controls
12	**Operations security**	(Seguretat de les operacions)	**7** Objectius, **14** Controls
13	**Communications security**	(Seguretat de les comunicacions)	**2** Objectius, **7** Controls
14	**System acquisition, development and maintenance**	(Seguretat en l'adquisició, desenvolupament i manteniment de sistemes d'informació)	**3** Objectius, **13** Controls
15	**Supplier relationships**	(Gestió de proveïdors)	**2** Objectius, **5** Controls
16	**Information security incident management**	(Gestió d'incidències)	**1** Objectiu, **7** Controls
17	**Information security aspects of business continuity management**	(Gestió de la continuïtat del negoci)	**2** Objectius, **4** Controls
18	**Compliance**	(Conformitat)	**2** Objectius, **8** Controls

S'agrupen les auditories segons si són internes, externes de 1a part o bé de tercera part (la de certificació del sistema, com a mínim) i s'agrupen en el Pla d'auditoria contemplant un període temporals de 3 anys de la forma:

3.2.4.1. Verificació/auditoria anual de la conformitat del sistema

Es contractarà a una entitat externa, si és possible la mateixa que ha realitzar l'auditoria de certificació, per a fer una auditora complerta de tot el sistema contra la norma ISO27001:2013.

El format de l'auditoria serà d'auditora interna (de primera part) però realitzada per una entitat externa per a donar-li independència i fiabilitat de cara a renovacions de la certificació de la norma.

L'equip auditor tindrà personal intern de l'organització ja que això contribuirà a la preparació tècnica i formació del personal en matèria d'auditoria. La qual cosa redundarà en la millora de les auditories internes fetes per personal de la pròpia organització. En especial ha de participar el responsable de seguretat dintre de l'equip d'auditoria.

L'**abast** de l'auditoria és la totalitat del SGSI de l'Ajuntament de Fita Alta.

L'auditoria anual es farà durant l'últim trimestre de l'any.

3.2.4.2. Auditories trimestrals

Revisió conjunta dels dominis que estan sota control i avaluació permanent per a aplicar criteris de millora contínua. Aquestes auditories revisaran el correcte funcionament dels controls dels dominis de seguretat.

L'**abast** d'aquestes auditories quedaria definit pels dominis següents:

- domini 8 – Gestió d'actius
- domini 9 – Control d'accés
- domini 10 – Criptografia
- domini 12 – Seguretat de les operacions
- domini 13 – Seguretat de les comunicacions
- domini 14 – Seguretat en l'adquisició, desenvolupament i manteniment dels sistemes d'informació
- domini 15 – Gestió d'incidències

Les auditories trimestrals es faran el 1r, 2n i 3r trimestres ja que el 4rt trimestre es fa la verificació anual de la conformitat del sistema.

Les auditories trimestrals les realitzarà personal intern amb un format d'auditoria interna i l'auditor en cap serà personal intern de l'Ajuntament. Els

dominis 10, 12, 13 i 15 requeriran la participació d'experts tècnics o fins i tot que col·laborí algun professional extern com a membre de l'equip d'auditoria.

3.2.4.3. Auditories anuals

Són auditories anuals específiques i realitzades de forma separada de dominis concrets. Dintre de les auditories que es realitzaran de forma anual se'n distingeixen 3 tipus diferents

3.2.4.3.1. Estat dels controls de la seguretat física i de l'entorn (domini 11)

La realitzarà personal intern amb format d'auditoria interna i el seu abast estaria restringit exclusivament a la seguretat física i de l'entorn i la informació que sobre ell hi pugui haver en qualsevol format.

3.2.4.3.2. Revisió del Pla de continuïtat i les seves proves (domini 17)

La realitzarà personal intern amb format d'auditoria interna i el seu abast estaria restringit exclusivament al Pla de Continuïtat del negoci la validació de les seves proves així com la informació que sobre ell hi pugui haver en qualsevol format.

3.2.4.3.3. Revisió conjunta dels dominis les característiques dels quals no tenen una variabilitat massa gran

Es acceptable per a aquests dominis no fer revisions amb més periodicitat.

- domini 5 – Política de seguretat
- domini 6 – Organització de la seguretat de la informació
- domini 7 – Seguretat relativa al personal
- domini 15 – Gestió de proveïdors
- domini 16 – Conformitat
- revisió del programa d'auditora.
  Aquest últim punt no és part de la norma però convé fer-ho en profunditat un cop a l'any de forma integrada amb al SGSI.

La combinació de totes aquestes auditories i la seva periodicitat, actuen amb l'objectiu conjunt de mantenir i millorar el sistema de gestió de la seguretat dels sistemes de TI. Es garanteix que els objectius bàsics del negoci es revisen de forma trimestral amb auditories internes i un cop a l'any són revisats per una entitat externa independent. Els aspectes més costosos de revisar o bé aquells que no tenen una variabilitat excessiva es revisen amb auditories internes de periodicitat anual.

El cicle del Pla d'auditoria ha de contemplar que cada 3 anys s'ha de substituir la auditoria de primera part realitzada per l'entitat externa per una auditoria de tercera part de certificació del seguiment de la norma amb l'objectiu de mantenir el sistema de gestió de la seguretat dels sistemes de TI certificat i vigent.

3.2.5. Model d'informe d'auditoria

El model d'informe d'auditoria dependrà del tipus d'auditoria realitzada i l'establiran a l'inici de l'auditoria el responsable de l'auditoria i l'equip auditor. En qualsevol cas, s'espera que contingui, com a mínim, els apartats següents:

- Introducció

Incorporà, com mínim, la data de l'auditoria i el nom de l'empresa i auditors que la realitzen i el tipus d'auditoria

- Abast de l'auditoria

Descripció de l'abast de l'auditoria. Detallant les àrees, departaments i/o processos auditats així com la relació dels controls de seguretat.

- Objectiu de l'auditoria

Detall dels objectius de l'auditoria

- Metodologia emprada

Descripció de la metodologia utilitzada per a la realització de l'auditoria fent referència als estàndards utilitzats. S'han d'explicar els objectius, les fases i les tècniques utilitzades.

- Resum executiu

Inclourà una introducció i les principals conclusions que s'hagin obtingut i les recomanacions principals que l'equip auditor pugui donar. Ha de ser breu i no ocupar més de dues pàgines.

- Conformitat del SGSI amb la norma o grau d'adequació

Aquest apartat s'ha d'incloure en el cas de la realització de l'auditoria de certificació o en les de revisió anual de la conformitat amb la norma.

- Detall de l'informe o llista detallada de les constatacions

Detall complert de les proves realitzades i les constatacions que s'han fet, especialment en el cas de les No-conformitats detectades.

Es recomana facilitar en fulls independents les constatacions independents i fer una avaluació de la importància o impacte que pot tenir a l'organització.

- Annexos

Qualsevol informació que doni suport a les constatacions de l'informe i que l'equip d'auditoria consideri que s'han de recollir i documentar.

- Recomanacions de millora

En el cas que l'auditori no sigui de certificació, l'equip auditor pot realitzar recomanacions de millora.

3.3. Gestió d'Indicadors

Es necessari definir indicadors per a que un sistema es mantingui viu i actualitzat o cal avaluar-ne l'eficàcia de manera continuada. Per a fer-ho s'han d'establir indicadors que permetin controlar el funcionament de les mesures de seguretat de la informació implantades, i l'eficàcia i l'eficiència que tenen, i definir els mecanismes i la periodicitat de mesura d'aquests indicadors.

L'efectivitat de l'SGSI està directament relacionada amb l'efectivitat dels controls implantats. Per a disposar d'informació sobre l'eficàcia dels controls, es imprescindible implantar indicadors que ens proporcionin aquesta informació.

Un indicador és una mesura respecte d'una referència. Tot indicador consta de vuit components bàsics:

1. **Nom de l'indicador**. Ha de ser un nom significatiu, no massa llarg, que doni idea de quin és el mesurament que es fa.
2. **Descripció de l'indicador**. Explicació de l'objectiu de mesura de l'indicador.
3. **Control de seguretat a què dóna suport**. A quin control o controls dóna cobertura
4. **Fórmula de mesurament**. Descripció de la fórmula aplicada per a obtenir la mesura. És important que els paràmetres que hi intervenen siguin concrets i no es prestin a ambigüitats.
5. **Unitats de mesura**. Les unitats de mesura han de ser especificades amb claredat.
6. **Freqüència de mesura**. Cada quant s'ha de recollir la mesura. La freqüència depèn de la variabilitat en el temps de la mesura.
7. **Valor objectiu i valor llindar**. Quan sigui possible dir quins és el valor correcte per a la companyia (valor objectiu) i quin és el valor per sota del qual s'ha d'aixecar una alarma (valor llindar).
8. **Responsable de la mesura**. Sobre quina persona o quin càrrec recau la responsabilitat de proporcionar el resultat de la mesura.

A l'hora d'indicar un indicador és important que el mesurament sigui fiable i repetible. Això vol dir que s'ha de basar en evidències objectives.

Hi ha diferents tipus d'indicadors. Posem uns exemples per indicar-los:

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

- **Indicadors d'operació**
  - Temps total de caiguda d'un determinat servei en l'últim mes
  - Nombre d'avaries d'equips informàtics en l'últim mes

- Trànsit mitja del tallafoc
- Nombre d'intents de penetració detectats per l'IDS respecte del nombre d'intents rebutjats
- Nombre de virus detectats respecte el nombre d'incidències per virus

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

Especificarem els indicadors basant-nos en els 14 dominis de la ISO/IEC 27001:2013 i dintre d'ells per a cada objectiu de control. Un cop especificats tots, podríem plantejar-nos fer una altra classificació dels mateixos segons si aquests són indicadors de gestió, d'operació o d'entorn.

La primera versió dels indicadors està basada en els controls i mètriques disponibles al portal de la ISO 27001 en espanyol http://iso27000.es/index.html

Es mostra un exemple dels indicadors per al domini "**Polítiques de seguretat de la Informació**" a l'objectiu "**Direcció de la gestió de la seguretat de la informació**".

3.3.1. Direcció de la gestió de la seguretat de la informació

Nom d'indicadors	**Cobertura de las polítiques**
Descripció	Percentatge de les seccions de l'ISO/IEC 27001/2 per a les quals s'han especificat, escrit, aprovat o publicat polítiques i les seves normes, procediments i directrius associades.
Control de seguretat	**5.1.1.** Conjunt de polítiques per a la seguretat de la informació
Fórmula de mesurament	Nombre de polítiques / normes especificades, escrites, aprovades o publicades
Unitats de mesura	Percentatge Nbre. Documents / Nbre. De seccions per a les que s'han d'especificar polítiques, normes, procediments i directrius
Freqüència de mesurament	Anual
Valor objectiu **Valor llindar**	90% 50%
Responsable de la mesura	Responsable de seguretat

Nom d'indicadors	**Grau de desplegament de les polítiques**
Descripció	Grau de desplegament i adopció de les polítiques al si de l'organització
Control de seguretat	**5.1.1**. Conjunt de polítiques per a la seguretat de la informació **5.1.2.** Revisió de les polítiques de seguretat de la informació
Fórmula de mesurament	Mesurat per auditoria, gerència o per auto-avaluació Percentatge d'aplicació de cada política, norma o procediment especificada.
Unitats de mesura	Percentatge
Freqüència de mesurament	Anual
Valor objectiu **Valor llindar**	100% 75%
Responsable de la mesura	Auditors si es mesura en auditoria Responsable de seguretat si és una revisió del comitè Responsables de l'aplicació de les polítiques mitjançant qüestionarid d'autoavaluació.

3.4. Procediment de Revisió per la Direcció

Serà missió del Comitè de Seguretat Corporativa la revisió anual de la Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La política serà aprovada per l'alcalde i difosa perquè la coneguin totes les parts afectades.

Les revisions del comitè de seguretat contemplaran els aspectes següents:

- Identificació en els nivells de risc, noves amenaces i vulnerabilitats.
- Identificació de canvis en l'organització
- Identificació de canvis en la legislació
- Revisió de l'estat del sistema i la seva implantació
- Anàlisi del compliment dels objectius de seguretat
- Anàlisi de l'efectivitat dels controls implantats i revisar l'evolució de l'estat de la seguretat
- Establir accions preventives, correctives i de millora

3.5. Gestió de Rols i Responsabilitats

L'Ajuntament de Fita Alta disposarà de dues estructures de gestió de la seguretat.

Estructura de Supervisió, que serà la responsable d'establir i aprovar els requisits de seguretat per al Sistema, a més a més de verificar i supervisar la correcta implementació i manteniment d'aquests requisits.

Estructura d'Operació, que serà la responsable de la implementació i manteniment dels requisits de seguretat.

3.5.1. Estructura de supervisió

3.5.1.1. Alcalde

Funcions:

- És responsable que l'Ajuntament de Fita Alta aconsegueixi els seus objectius de seguretat TIC a curt, mitjà i llarg termini. Actua en funció d'alta direcció.
- Ha de donar suport explícitament i amb notorietat de les activitats de seguretat TIC a l'Ajuntament.
- Ha d'expressar les seves inquietuds al Comitè de Seguretat Corporativa per mitjà del Responsable de Seguretat Corporativa.
- Aprova la Política de Seguretat de l'Ajuntament de Fita Alta.
- Aprova els pressupostos presentats pel Comitè de Seguretat Corporativa quan superen una determinada quantitat.
- Aprova el Pla Director de l'ENS, que recull els principals projectes i iniciatives en matèria de seguretat.
- Nomena els membres del Comitè de Seguretat Corporativa

3.5.1.2. Comitè de Seguretat Corporativa

Funcions:

- Coordina totes les funcions de seguretat de l'Ajuntament de Fita Alta.
- Vetlla pel compliment de la normativa d'aplicació legal, regulatòria i sectorial.
- Vetlla per l'alineament de les activitats de seguretat i els objectius TIC de l'Ajuntament de Fita Alta.
- És responsable de l'elaboració de la Política de Seguretat.
- Si existeixen, ha d'aprovar les polítiques de seguretat específiques de les àrees.
- Coordina i aprova les propostes rebudes de projectes dels diferents àmbits de seguretat.
- Rep les inquietuds de l'Alta Direcció i les transmet als Responsables de la informació dels Serveis.
- És responsable de la creació i aprovació de les normes per l'ús dels serveis TIC.
- Ha d'aprovar els procediments d'actuació per l'ús dels serveis TIC.

- Recull informes de l'estat de seguretat de l'Ajuntament de Fita Alta i de possibles incidents que li fan arribar els Responsables de la informació dels Serveis.
- Coordina i dóna respostes a les inquietuds transmeses pels diferents Responsables de la informació dels Serveis.
- Assignar els rols dins de la Política de Seguretat.
- Ha d'aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de les TIC.
- Ha d'assessorar-se sobre aquells temes que hagi de decidir o emetre una opinió.

3.5.2. Estructura d'operació. Rols

3.5.2.1. Responsables de la informació del Serveis

Són els responsable últims de l'ús que es faci d'una certa informació d'un Servei i, per tant, de la seva protecció.

Són els responsable últims de qualsevol error o negligència que provoqui un incident de confidencialitat o d'integritat.

Tenen la potestat d'establir els requisits de la informació en matèria de seguretat, és a dir, determinar els nivells de seguretat de la informació, amb l'assessorament del responsable de seguretat corporativa i del responsable del sistema.

Són els responsables de determinar els nivells de seguretat dels actius, en cada dimensió de seguretat, amb l'assessorament del responsable de seguretat corporativa i del responsable del sistema.

3.5.2.2. Responsable de seguretat Corporativa

És l'autoritat designada per l'Ajuntament de Fita Alta segons el procediment descrit en aquesta política de seguretat.

Funcions:

- Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes TIC en el seu àmbit de responsabilitat.
- Realitzar o promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació STIC dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació manejada i els serveis prestats.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat del sistema.
- Monitoritzar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria implementats en el sistema.

- Donar suport i supervisar la investigació dels incidents de seguretat des de la notificació fins a la seva resolució.
- Elaborar l'informe periòdic de seguretat per al propietari del sistema, incloent els incidents més rellevants del període.
- Actua com a Secretari del Comitè de Seguretat Corporativa.
- Convoca el Comitè de Seguretat Corporativa.
- Rep les inquietuds de l'Alta Direcció i dels Responsables de Seguretat, per discutir-les en les reunions del Comitè de Seguretat Corporativa.
- Ha d'estar informat dels canvis normatius, de les possibles conseqüències, posar-ho en coneixement del Comitè de Seguretat Corporativa proposant mesures d'adequació.
- Ha d'estar alerta dels canvis de la tecnologia que disposa l'Ajuntament de Fita Alta, i de les conseqüències d'aquests canvis, proposant les mesures oportunes.
- Responsable de la presa de decisions del dia a dia, entre reunions del Comitè de Seguretat Corporativa.
- Coordinar totes les actuacions relacionades amb la seguretat de l'Ajuntament de Fita Alta en cas de desastre.
- És el responsable de la redacció dels procediments d'actuació en l'ús dels serveis TIC .
- És el responsable de la correcta execució de les instruccions del Comitè de Seguretat Corporativa.
- És el responsable de la presentació periòdica dels informes sobre l'estat de la seguretat dels serveis TIC al Comitè de Seguretat Corporativa.
- És responsable de la preparació d'informes en cas d'incidències molt greus.
- És responsable de l'elaboració d'un anàlisi de riscos dels sistemes TIC, que ha d'actualitzar periòdicament.
- És responsable de l'execució regular de verificacions de seguretat i, si cal, proposarà mesures correctores.
- És responsable de l'elaboració i seguiment del Pla de Seguretat.
- Ha d'elaborar els requisits de formació i qualificació d'administradors, operadors i usuaris.
- És responsable de la identificació de tasques d'administració i operació que garanteixin la satisfacció dels criteris i requisits de segregació de tasques imposades pel Comitè de Seguretat Corporativa.
- És l'interlocutor oficial en comunicacions amb altres entitats.
- És el responsable de coordinar la resposta davant incidents que desbordin els casos previstos i procedimentats, i de coordinar la investigació forense relacionada amb incidents considerats rellevants.

3.5.2.3. Responsable del sistema

El responsable del sistema té les següents funcions en relació amb la seguretat:

- Desenvolupar, operar i mantenir del sistema durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i política de gestió del sistema establint els criteris d'ús i els serveis disponibles en aquest.

- Definir la política de connexió o desconnexió d'equips i usuaris nous al sistema.
- Aprovar els canvis que afectin la seguretat de la manera d'operació del sistema.
- Decidir les mesures de seguretat que s'aplicaran als subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova del mateix.
- Implantar i controlar les mesures específiques de seguretat del sistema i assegurar-se que aquestes s'integrin adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada de maquinari i programari a utilitzar en el sistema.
- Aprovar qualsevol modificació substancial de la configuració de qualsevol element del sistema.
- Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema.
- Determinar la categoria del sistema segons el procediment descrit en l'annex I del ENS i determinar les mesures de seguretat que s'han d'aplicar segons es descriu en l'annex II del ENS.
- Elaborar i aprovar la documentació de seguretat del sistema.
- Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.
- Vetllar pel compliment de les obligacions de l'administrador de seguretat del sistema.
- Investigar els incidents de seguretat que afecten el sistema, i si escau, comunicació al responsable de Seguretat o a qui aquest determini.
- Establir plans de contingència i emergència, portant a terme freqüents exercicis perquè el personal es familiaritzi amb ells.
- A més, el responsable del sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si és informat de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsable de la informació afectada, del servei afectat i el responsable de seguretat, abans de ser executada.
- Responsable de la implantació, configuració i manteniment dels serveis de seguretat relacionats amb les TIC.
- Ha d'executar els procediments rutinaris i aquells assignats per la resolució d'incidents.
- Ha de reportar qualsevol inseguretat o debilitat al Responsable de Seguretat.

3.5.2.4. Operadors de seguretat

Funcions en relació amb la seguretat:

- L'elaboració, quan així ho determini el responsable del sistema, aplicació i gestió dels Procediments Operatius de Seguretat.
- La gestió, configuració i actualització, si s'escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del sistema.
- Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema.

- Informar als Responsable de Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Aprovar els procediments locals de control de canvis en la configuració vigent del sistema.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que són aplicats els procediments aprovats per al maneig del sistema.
- Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta.
- Establir procediments de seguiment i reacció davant alarmes i Situacions imprevistes.
- Iniciar el procés de resposta davant incidents que es produeixin en el sistema sota la seva responsabilitat, informant i col·laborant amb el Responsable de Seguretat en la investigació d'aquests.

3.5.2.5. Comitè de seguretat TIC

Es crearà internament un comitè en el servei que presta els serveis TIC, per tal de coordinar les actuacions en matèria de seguretat TIC d'acord a aquesta política de seguretat i de les instruccions del Comitè de Seguretat Corporativa.

Estarà format almenys pel responsable de seguretat, responsable de sistema i operadors de seguretat.

3.5.2.6. Usuaris

Funcions:

- Es relacionen amb les TIC per a complir les seves obligacions laborals.
- Es fonamental la seva conscienciació en la seguretat de les TIC pel manteniment de la seguretat del Sistema.
- Han d'estar informats de les seves obligacions i responsabilitats i haver estat correctament instruïts per les tasques que realitzin.
- Són responsables de conèixer els procediments de la seva competència
- Són responsables d'informar de qualsevol incident de seguretat que sigui observat durant l'operació del seu Sistema.

3.5.3. Procediments de designació

El responsable de Seguretat serà nomenat per l'alcalde a proposta del Comitè de Seguretat Corporativa.

El responsable del departament que presti un servei o disposi d'informació per mitjans electrònics serà el Responsable de la informació d'aquest Servei, d'acord a les funcions i responsabilitats dins el marc establert per aquesta Política.

3.6. Metodologia d'Anàlisi de Riscos

La anàlisi de riscos és la primera fase que s'ha d'analitzar quan es vol implantar un SGSI. Serveix per a descobrir quines necessitats de seguretat té l'organització després de detectar quins són els nostres forats de seguretat i les amenaces a les que estem exposats. L'anàlisi de riscos ens permet realitzar la gestió de riscos, que consisteix a triar la millor solució de seguretat per a afrontar els riscos a que està exposada l'organització i que alhora permet assolir els seus objectius.

L'anàlisi de riscos, des del punt de vista de la seguretat, correspon al procés d'identificació d'aquests riscos: en determina la magnitud i n'identifica les àrees que requereixen mesures de protecció.

Actualment hi ha diferents metodologies vàlides per a fer una anàlisi de riscos. Cadascuna d'aquestes metodologies té una sèrie de característiques pròpies, però bàsicament es fonamenten totes en els mateixos processos i treballen sobre els mateixos elements.

- **Actius** : elements que s'han de protegir
- **Amenaces** : situacions de que s'han de protegir els actius
- **Vulnerabilitats** : aspectes que faciliten la materialització de les amenaces
- **Impactes** : conseqüències que es produeixen a l'organització quan una amenaça aprofita una vulnerabilitat per a danyar un actiu

El risc és la relació que hi ha entre aquests quatre elements. Combinant-los entre si s'obtenen els diferents tipus de riscos a que està exposada una organització.

Els motius pels quals s'ha de fer una anàlisi de riscos són:

- Permet identificar els riscos a què està exposada l'organització des del punt de vista de la seguretat i que poden afectar el desenvolupament de les activitats de negoci de l'organització.
- Permet a l'organització fer una selecció de les mesures de seguretat que s'hi han d'implantar.
- Permet fer i elaborar els plans de contingències d'una organització. Això vol dir que una anàlisi de risc ens presentarà les situacions que poden provocar una incidència de seguretat i que, alhora, no es poden reduir implantant les mesures de seguretat.
- Les organitzacions que tinguin previst implantar les diferents normatives de seguretat (ISO 27001) i crear un sistema de gestió de la seguretat de la informació (SGSI), amb la intenció d'aconseguir certificar-lo, han de tenir una anàlisi de riscos, que és el punt de partida de tot el procés de certificació.

3.6.1. Metodologia MAGERIT

MAGERIT és la Metodologia d'Anàlisi i Gestió de Riscos Elaborada pel Consell Superior d'Administració Electrònica, com a resposta a la percepció de que l'administració, i, en general, la tota La societat, depenen de forma Creixent de les Tecnologies de la Informació per al compliment de la seva Missió.

La Raó de Ser de MAGERIT està directament relacionada amb la generalització de l'ús de les tecnologies de la Informació, que suposa uns beneficis evidents per als ciutadans; però també dóna peu a certs riscos que s'han de minimitzar amb mesures de seguretat que generin confiança.

MAGERIT Interessa a tots aquells que treballen amb informació digital i sistemes informàtics per a tractar-la. Si la Informació, o els serveis que es presten gràcies a ella, són valuosos, MAGERIT els permetrà saber quin és el seu valor i ens ajudarà a protegir-lo. Conèixer el Risc a què estan sotmesos els elements de treball és Imprescindible per poder gestionar-los. MAGERIT segueix una aproximació metòdica que no deixa lloc a la improvisació ni depèn de l'arbitrarietat de l'analista.

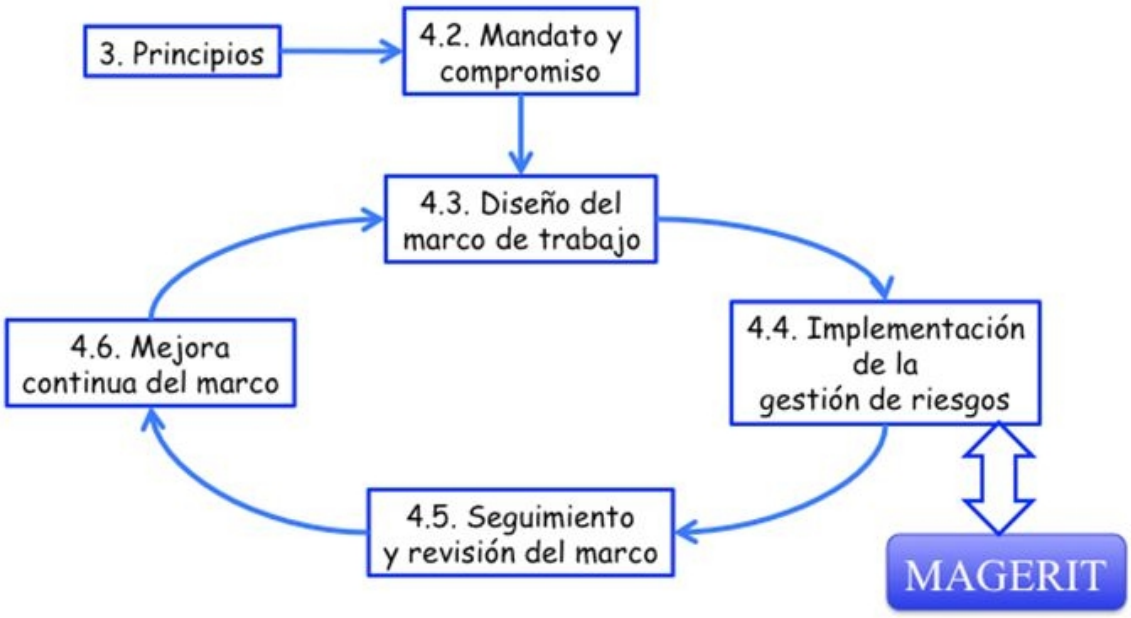


Figura - ISO 31000 – Marc de treball per a la gestió de riscos

L'anàlisi i gestió dels riscos és un aspecte clau del Reial Decret 3/2010, de 8 de gener , pel que es regula l'esquema nacional de seguretat (en endavant ENS) en l'àmbit de l'administració electrònica que té la finalitat de donar compliment al principi de proporcionalitat en el compliment dels principis bàsics i requisits mínims per a la protecció adequada de la informació. MAGERIT és un instrument per facilitar la implantació i aplicació de l'Esquema Nacional de Seguretat.

Donat que Fita Alta és un Ajuntament i, per tant, una administració pública, està obligada al compliment normatiu de l'ENS. Aquest és el motiu principal pel qual la metodologia d'anàlisi de riscos que seguirem és MAGERIT ja que tot i haver estat dissenyada per a donar compliment a l'ENS dintre de la normativa espanyola també segueix els principis de les normatives internacionals reflectides a la ISO/IEC 27001:2013.

Hi ha una eina dissenyada pel "Centro Criptológico Nacional" (en endavant CCN-CERT) que permet automatització de la metodologia MAGERIT i la seva aplicació d'una forma directa. Aquesta eina, anomenada PILAR, permet la realització d'una anàlisi de riscos. Hi ha diferents versions de l'eina PILAR que es poden utilitzar tant per a la realització d'una anàlisi de riscos orientada a donar compliment a la norma ISO/IEC 27001:2013 com si es vol donar compliment a l'ENS.

La possibilitat de fer una anàlisi de riscos de les dues normatives que volem que compleixi l'Ajuntament de Fita Alta (ENS i ISO/IEC 27001:2013) fan que sigui PILAR l'eina que utilitzarem per a realitzar-la.

3.6.2. Eina EAR-PILAR del CCN-CERT

Les eines EAR (Entorn d'Anàlisi de Riscos) suporten l'anàlisi i la gestió de riscos d'un sistema d'informació seguint la metodologia MAGERIT (metodologia d'anàlisi i gestió de riscos dels sistemes d'informació) i ESTÀ desenvolupada i finançada parcialment pel CCN . S'actualitzen periòdicament i ha diverses variants :

- **PILAR**: versió íntegra de l'eina
- **PILAR Basic**: versió senzilla per a Pymes i Administració Local
- **µPILAR**: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos

3.6.2.1- Metodologia

Els actius estan exposats a amenaces que quan es materialitzen degraden l'actiu produint un impacte a l'organització. Si estimem la freqüència amb que es materialitzen les amenaces podem deduir el risc a que aquesta exposat el sistema.

La degradació i la freqüència qualifiquen la vulnerabilitat del sistema. El gestor del sistema d'informació disposa de salvaguardes, que o bé redueixen la freqüència d'ocurrència, o bé redueixen o limiten el seu impacte. Depenent del grau d'implantació de aquestes salvaguardes, el sistema passa un una nova estimació de risc anomenada "risc residual".

Pilar disposa d'una biblioteca estàndard de propòsit general capaç de realitzar qualificacions de seguretat de normes com són:

- **ISO/IEC 27002** (2005, 2013) - Codi de Bones Pràctiques per a la Gestió de la Seguretat de la Informació
- **ENS** - Esquema Nacional de Seguretat

Totes les eines es poden descarregar des de la pàgina del CCN-CERT
https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

3.6.2.2. PILAR

S'analitzen els riscos en diverses dimensions: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat (accountability). Per al tractament del risc es proposen:

- Salvaguardes (o contramesures)
- Normes de seguretat
- Procediments de seguretat

La versió íntegra de PILAR també contempla l'anàlisi d'impacte i continuïtat d'operacions. S'analitza l'efecte de les interrupcions de servei tenint en compte la durada de la interrupció. Per al tractament d'aquest risc es proposen:

- Salvaguardes (o contramesures)
- Còpies de seguretat)
- Plans de recuperació de desastres

L'anàlisi permet avaluar i analitzar el risc residual resultant .

3.6.2.3. PILAR-Bàsic

És una versió senzilla per a PIME i Administració local. Com en el cas de la versió íntegra, S'analitzen els riscos en diverses dimensions: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat (accountability).

Per al tractament del risc es proposen salvaguardes (o contramesures), analitzant el risc residual.

3.6.2.4. µPILAR

És l'eina PILAR reduïda a la mínima expressió per la realització d'una anàlisi de riscos molt ràpida. El resultat de l'anàlisi es pot carregar a PILAR per a un estudi més detallat.

µPILAR ES distribueix amb perfils específics (ISO 27000 o ENS) i només es poden analitzar els perfils de la distribució.

S'analitzen els riscos en diverses dimensions: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat (accountability).

Per tractar el risc es proposen salvaguardes (o contramesures) , analitzant el risc residual.

3.7. Declaració de Aplicabilitat

La declaració d'aplicabilitat recull la relació de controls de l'ISO 27002:2013 especificant per a cadascun d'ells si és o no aplicable al SGSI de l'Ajuntament de Fita Alta. En cas de ser aplicable s'adjunta una descripció de la forma en que s'implementarà el control. En el cas que el control no sigui aplicable s'ha de justificar de la seva exclusió.

La descripció del control en la majoria de casos està extreta o és un resum del que es defineix a la guia de l' ISO 27002:2013. També s'adjunta a l'Annex V l'informe de declaració d'aplicabilitat extret de l'eina PILAR.

3.7.1. - A.5 polítiques de seguretat de la informació

Aplicable?					Aplicable?	Descripció del control
	A.5 POLÍTIQUES DE SEGURETAT DE LA INFORMACIÓ					
	A.5.1 Directrius de la Direcció en Seguretat de la informació					
Sí			A.5.1.1	Document de Política de seguretat de la informació	Sí	Tota organització ha de tenir una normativa comuna de seguretat que reguli les línies mestres sobre la forma de treballar de tota l'organització en matèria de seguretat.
Sí			A.5.1.2	Revisió de la política de seguretat de la informació	Sí	Les polítiques s'han de revisar de forma periòdica per a garantir la seva vigència.

3.7.2. - A.6 aspectes organitzatius de la seguretat de la informació

A.6 ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ					
	A.6.1 Organització interna				
		A.6.1.1	Assignació de responsabilitats per a la seguretat de la informació	Sí	Tot el personal de l'organització i els seus col·laboradors (proveïdors, personal extern, eetc.) han de saber les responsabilitats que tenen envers de la protecció de la informació.
		A.6.1.2	Segregació de tasques	Sí	Les àrees conflictives o amb especial responsabilitat han d'estar segregades per a reduir les d'accessos no autoritzats o modificacions no desitjades o incorrectes en la configuració dels actius.
		A.6.1.3	Contacte amb les autoritats	Sí	S'han de definir procediments que especifiquin quan, com i a quines autoritats s'ha de contactar en el cas de produir-se incidents de seguretat.
		A.6.1.4	Contacte amb grups d'interès especial	Sí	S'ha de mantenir contacte amb fòrums i especialistes de seguretat de la informació
		A.6.1.5	Seguretat de la informació en la gestió de projectes	Sí	Tots els projectes han de contemplar i incorpora la gestió de la seguretat de la informació.
	A.6.2 Dispositius mòbils I teletreball				
		A.6.2.1	Política d'ús de dispositius per a la mobilitat	Sí	S'han de definir polítiques que gestionin els nous riscos derivats de la utilització de dispositius mòbils
		A.6.2.2	Teletreball	Sí	S'han de definir polítiques per a gestionar i protegir la informació que es utilitzada en els centres o serveis de teletreball.

3.7.3. - A.7 seguretat relativa al personal

A.7 SEGURETAT RELATIVA AL PERSONAL					
	A.7.1 Abans de la contractació				
		A.7.1.1	Investigació dels antecedents	Sí	Verificar que els antecedents del personal contractat és adequat per al nivell de responsabilitat del nivell de seguretat de la informació que ha de gestionar.
		A.7.1.2	Termes i condicions de la contractació	Sí	Garantir que els contractes recullen les obligacions dels treballadors i empreses terceres referents a la segurerat de la informació.
	A.7.2 Durant la contractació				
		A.7.2.1	Supervisió d'obligacions	Sí	Garantir que tot el personal aplica la seguretat de la informació seguint les polítiques i procediments de l'organització.
		A.7.2.2	Conscienciació, educació i capacitació en seguretat de la informació	Sí	Tot el personal de l'organització ha de rebre formació sobre seguretat de la informació relacionada i adequada al seu lloc de treball.
		A.7.2.3	Procés disciplinari	Sí	Ha d'existir un procediement formal i conegut per a sancionar al personal que hagi produït una fuita d'informació o hagi generat de forma conscient un incident de seguretat.
	A.7.3 Cesament o canvi del lloc de treball				
		A.7.3.1	Cesament o canvi del lloc de treball	Sí	S'han de definir procediments que garanteixin que el procés de canvi de funcions o de sortida de l'organització o finalització de contracte també reassigna o denega a la personal els drets d'accés físics i lògics que tenia en la seva situació laboral anterior.

3.7.4. - A.8 gestió d'actius

A.8 GESTIÓ D'ACTIUS					
	A.8.1 Responsabilitat sobre els actius				
		A.8.1.1	Inventari d'actius	Sí	Cal tenir un inventari actualitzat dels actius per a poder desenvolupar i mantenir l'activitat i definir-ne els responsables.
		A.8.1.2	Propietat dels actius	Sí	Tots els actius inclosos al l'inventari han de tenir un responsable de la seva protecció i de la informació que s'hi gestiona.
		A.8.1.3	Ús acceptable dels actius	Sí	Ha d'existir i fer-se públic un document que defineixi les normes del que es considera un ús acceptable de la informació i dels actius i equipaments informàtics per part del personal.
		A.8.1.4	Retorn dels actius	Sí	Tot els treballadors o personal extern ha de retornar els actius propietat de l'organització quan finalitzi el seu contracte o relació contractual amb l'organització.
	A.8.2 Classificació de la informació				
		A.8.2.1	Directrius de classificació	Sí	Cal definir les directrius de la classificació de la informació per a poder definir el seu nivell de protecció segons el seu valor, criticitat i sensibilitat per a l'organització respecte a accessos no autoritzats o la seva revelació.
		A.8.2.2	Etiquetat i manipulació de la informació	Sí	S'han de definir procediments per a l'etiquetat de la informació d'acord amb les directrius de classificació adoptades per l'organització.
		A.8.2.3	Manipulació dels actius	Sí	Els procediments de manipulació s'han d'implantar de forma coherent amb la classificació de la informació adoptada per l'organització.
	A.8.3 Manipulació dels suports d'emmagatzemament				
		A.8.3.1	Gestió dels suports extraïbles	Sí	S'han de definir procediments per a la gestió dels suports extraïbles d'acord amb les directrius de classificació adoptades per l'orgnanització.
		A.8.3.2	Eliminació de suports	Sí	Els dispositius o suports s'han d'eliminar seguint uns procediments formals que quan deixin de ser utilitzats de forma que es minimitzi el risc de fuita d'informació confidencial.
		A.8.3.3	Suports físics en trànsit	Sí	Els dispositius físics en trànsit s'han de protegir contra accessos no autoritzats, usos inadequats o corrupció de la informació durant el seu transport.

3.7.5. - A.9 control d'accessos

A.9 CONTROL D'ACCESSOS					
	A.9.1 Requeriments de negoci per al control d'accessos				
		A.9.1.1	Política de control d'accessos	Sí	Tota organització ha de tenir una normativa que defineixi l'accés a la informació i als recursos tenint en consideració el requisits del negoci i de seguretat de la informació.
		A.9.1.2	Control d'accessos a les xarxes i els serveis associats	Sí	Els usuaris només han de tenir accés als serveis de xarxa per als quals hagin estat autoritzats.
	A.9.2 Gestió d'accés de l'usuari				
		A.9.2.1	Gestió d'altes/baixes en el registre d'usuaris	Sí	S'ha de definir un procés de registre d'altes i de baixes que habiliti els usuaris als quals es poden donar accés als recursos dels sistemes. Els usuaris han de tenir associat un identificador personal i han de passar per un procés d'identificacií i autenticació.
		A.9.2.2	Gestió dels drets d'accés assignats als usuaris	Sí	Definició del procés d'assignació i/o revocació d'accés dels usuaris a tots els sistemes i serveis.
		A.9.2.3	Gestió dels drets d'accés amb privilegis especials	Sí	L'Assignació i ús de privilegis especials s'ha de fer de forma restringida i controlada amb un procediment especial en concordancia amb el que es defineixi a la política de control d'accessos.
		A.9.2.4	Gestió d'informació confidencial d'autenticació d'usuaris	Sí	L'assignació de la informació d'autenticació i el deure de mantenir-la en secret s'ha de realitzar mitjançant un procés formal. Els usuaris han de conéixer els codis de bones pràctiques i normés de bon d'ús de les estacions de treball i dels sistemes d'accés a la informació.
		A.9.2.5	Revisió dels drets d'accés dels usuaris	Sí	S'han de fer revisions periòdiques sobre els permisos i privilegis d'accés dels usuaris a cada recurs.
		A.9.2.6	Retirada o adaptació dels drets d'accés	Sí	Els drets d'accés als recursos i serveis del personal propi o extern s'han d'eliminar quan hi ha una finalització de contracte o adaptar-lo a les noves condicions contractuals en cas que aquestes es produeixin.
	A.9.3 Responsabilitats de l'usuari				
		A.9.3.1	Ús de la informació confidencial per a l'autenticació	Sí	Els usuaris han de ser advertits que no poden divulgar ni compartir la informació d'autenticació i que aquesta és considerada com a informació confidencial fent-se responsables del seu manteniment en secret.
	A.9.4 Control d'accés a sistemes i aplicacions				
		A.9.4.1	Restricció de l'accés a la informació	Sí	Les polítiques de control d'accés defineixen les restriccions d'accés a la informació.
		A.9.4.2	Procediments segurs d'inici de sessió	Sí	L'accés als sistemes i les aplicacions ha de ser realitzat utilitzant procediments segurs d'inici de sessió quan així ho requereixin les polítiques de control d'accés.
		A.9.4.3	Gestió de les contrasenyes d'usuari	Sí	Els sistemes de gestió de passwords ha de ser interactiu i garantir que els passwords que es fan servir són robustos i de qualitat.
		A.9.4.4	Ús de les eines d'administració de sistemes	Sí	L'ús d'eines d'administració de sistemes ha d'estar fortament controlat i ha de deixar constància del seu ús en fitxers de log.
		A.9.4.5	Control d'accés al codi font dels programes	Sí	L'accés al codi font dels programes ha d'estar restringit.

3.7.6. - A.10 xifrat / criptografia

A.10 XIFRAT / CRIPTOGRAFIA					
	A.10.1 Controls criptogràfics				
		A.10.1.1	Política d'ús dels controls criptogràfics	Sí	S'ha de desenvolupar i implantar una política d'ús de sistemes criptogràfics i de xifrat per a protegir la informació.
		A.10.1.2	Gestió de claus	Sí	La política d'ús dels controls criptogràfics ha de contemplar tot el cicle de vida de la gestió de les claus criptogràfiques incloent la generació, l'emmagatzemament, l'accés, distribució i retirada i destrucció de les claus.

3.7.7. - A.11 seguretat física i ambiental

A.11 SEGURETAT FÍSICA I AMBIENTAL					
	A.11.1 Àrees segures				
		A.11.1.1	Perímetre de seguretat física	Sí	S'han d'adoptar mesures per a controlar l'accés físic a edificis i sales que continguin instal·lacions de processament o informació sensible o crítica per a l'organització.
		A.11.1.2	Controls físics d'entrada	Sí	Les àrees segures han d'estar protegides amb controls físics d'accés al qual només pugui accedir el personal autoritzat.
		A.11.1.3	Seguretat d'oficines, despatxos i recursos	Sí	S'han d'adoptar mesures de seguretat per a l'accés a les oficines, despatxos i recursos.
		A.11.1.4	Protecció contra les amenaces externes i ambientals	Sí	S'han d'adoptar mesures per a protegir-se de desastres naturals, atacs maliciosos o accidents.
		A.11.1.5	El treball en àrees segures	Sí	S'han de desenvolupar procediment per a treballar amb àrees segures dotades d'una seguretat perimetral.
		A.11.1.6	Àrees d'accés públic, càrrega i descàrrega	Sí	Les zones o àrees d'accés públic on pot accedir personal no autoritzat han de ser controlades i si és possible estar aïllades d'instal·lacions de procés de dades per a evitar accessos no autoritzats. (En el nostre cas foren les oficines d'atenció al públic).
	A.11.2 SEGURETAT DELS EQUIPS				
		A.11.2.1	Emplaçament i protecció d'equips	Sí	Els equips han d'estar ubicats i protegits per a reduir els riscos d'amenaces ambientals i altres perills
		A.11.2.2	Subministrament de serveis públics	Sí	Els equips han d'estar protegits davant d'interrupcions de subministrament de serveis públics per part de les empreses proveïdores
		A.11.2.3	Seguretat del cablejat	Sí	El cablejat elèctric i de telecomunicacions que doni serveis de dades ha d'estar protegit contra intercepcions, interferències o danys.
		A.11.2.4	Manteniment dels equips	Sí	Els equips s'han de mantenir correctament per a garantir la seva disponibilitat i integritat.
		A.11.2.5	Retirada i eliminació dels equips	Sí	La retirada i eliminació dels equips no pot fer-se sense autorització prèvia i s'ha de realitzar seguint el procediment desenvolupat per a aquests casos.
		A.11.2.6	Seguretat dels equips i actius fora de les instal·lacions	Sí	S'han d'aplicar mesures de seguretat addicionals als equips i actius que estiguin fora de l'organització per a protegir la confidencialitat de la informació i evitar els accessos no autoritzats.
		A.11.2.7	Reutilització o retirada segura de dispositius d'emmagatzemament	Sí	Abans de reutilitzar qualsevol equipament o retirar-lo d'ús s'ha de verificar que qualsevol informació confidencial o sensible que pugui haver en els seus dispositius d'emmagatzemament és destruïda, esborrada i sobreescrita utilitzant tècniques que facin irrecuperable la informació original.
		A.11.2.8	Equip informàtic d'usuari desatès	Sí	Els usuaris han de garantir que els seu equipament d'usuari quan ells no hi són queda convenientmen protegit.
		A.11.2.9	Política de lloc de treball net i bloqueig de pantalla	Sí	S'han d'adoptar polítiques d'escriptori net de papers i dispositius extraïbles i bloqueig de pantalles.

3.7.8. - A.12 seguretat en l'operativa

A.11 SEGURETAT FÍSICA I AMBIENTAL					
	A.11.1 Àrees segures				
		A.11.1.1	Perímetre de seguretat física	Sí	S'han d'adoptar mesures per a controlar l'accés físic a edificis i sales que continguin instal·lacions de processament o informació sensible o crítica per a l'organització.
		A.11.1.2	Controls físics d'entrada	Sí	Les àrees segures han d'estar protegides amb controls físics d'accés al qual només pugui accedir el personal autoritzat.
		A.11.1.3	Seguretat d'oficines, despatxos i recursos	Sí	S'han d'adoptar mesures de seguretat per a l'accés a les oficines, despatxos i recursos.
		A.11.1.4	Protecció contra les amenaces externes i ambientals	Sí	S'han d'adoptar mesures per a protegir-se de desastres naturals, atacs maliciosos o accidents.
		A.11.1.5	El treball en àrees segures	Sí	S'han de desenvolupar procediment per a treballar amb àrees segures dotades d'una seguretat perimetral.
		A.11.1.6	Àrees d'accés públic, càrrega i descàrrega	Sí	Les zones o àrees d'accés públic on pot accedir personal no autoritzat han de ser controlades i si és possible estar aïllades d'instal·lacions de procés de dades per a evitar accessos no autoritzats. (En el nostre cas foren les oficines d'atenció al públic).
	A.11.2 SEGURETAT DELS EQUIPS				
		A.11.2.1	Emplaçament i protecció d'equips	Sí	Els equips han d'estar ubicats i protegits per a reduir els riscos d'amenaces ambientals i altres perills
		A.11.2.2	Subministrament de serveis públics	Sí	Els equips han d'estar protegits davant d'interrupcions de subministrament de serveis públics per part de les empreses proveïdores
		A.11.2.3	Seguretat del cablejat	Sí	El cablejat elèctric i de telecomunicacions que doni serveis de dades ha d'estar protegit contra intercepcions, interferències o danys.
		A.11.2.4	Manteniment dels equips	Sí	Els equips s'han de mantenir correctament per a garantir la seva disponibilitat i integritat.
		A.11.2.5	Retirada i eliminació dels equips	Sí	La retirada i eliminació dels equips no pot fer-se sense autorització prèvia i s'ha de realitzar seguint el procediment desenvolupat per a aquests casos.
		A.11.2.6	Seguretat dels equips i actius fora de les instal·lacions	Sí	S'han d'aplicar mesures de seguretat addicionals als equips i actius que estiguin fora de l'organització per a protegir la confidencialitat de la informació i evitar els accessos no autoritzats.
		A.11.2.7	Reutilització o retirada segura de dispositius d'emmagatzemament	Sí	Abans de reutilitzar qualsevol equipament o retirar-lo d'ús s'ha de verificar que qualsevol informació confidencial o sensible que pugui haver en els seus dispositius d'emmagatzemament és destruïda, esborrada i sobreescrita utilitzant tècniques que facin irrecuperable la informació original.
		A.11.2.8	Equip informàtic d'usuari desatès	Sí	Els usuaris han de garantir que els seu equipament d'usuari quan ells no hi són queda convenientmen protegit.
		A.11.2.9	Política de lloc de treball net i bloqueig de pantalla	Sí	S'han d'adoptar polítiques d'escriptori net de papers i dispositius extraïbles i bloqueig de pantalles.

3.7.9. - A.13 seguretat en les telecomunicacions

A.13 SEGURETAT EN LES TELECOMUNICACIONS					
	A.13.1 Gestió de la seguretat en les xarxes				
		A.13.1.1	Controls de xarxa	Sí	Gestionar correctament les xarxes i les infraestructures per a garantir la protecció de la informació i l'accés a ls serveis i als recursos.
		A.13.1.2	Mecanismes de seguretat associats als serveis en xarxa	Sí	Els mecanismes de seguretats s'han d'incorporar en els serveis en xarxa i incloure'ls en els acords de servei contractats tant si són prestats en la mateixa organització com si estan externalitzats.
		A.13.1.3	Segregació de xarxes	Sí	Els diferents serveis d'informació, sempre que sigui possible, s'han de segregar en diferents xarxes per a poder aplicar diferents polítiques de gestió de riscos sobre les diferents xarxes segregades.
	A.13.2 Intercanvis d'informació amb terceres parts (externes)				
		A.13.2.1	Polítiques i procediments d'intercanvi d'informació	Sí	Definició de polítiques i procediments per a protegir els intercanvis d'informació mitjançant eines de comunicació.
		A.13.2.2	Acords d'intercanvi	Sí	S'han de realitzar acords que garanteixin un intercanvi segur d'informació entre l'organització i terceres parts.
		A.13.2.3	Missatgeria electrònica	Sí	S'han de prendre mesures per a protegir la informació utilitzada en missatgeria electrònica
		A.13.2.4	Acords de confidencialitat i de secret	Sí	Els acords de confidencialitat i de secret s'han d'identificar, documentar i revisar de forma periòdica.

3.7.10. - A.14 adquisició, desenvolupament i manteniment dels sistemes d'informació

A.14 ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ					
	A.14.1 Requisits de seguretat dels sistemes d'informació				
		A.14.1.1	Anàlisi i especificació dels sistemes d'informació	Sí	La seguretat s'ha de considerar en tot el cicle de vida de desenvolupament de sistemes: anàlisi de requisits i viabilitat, disseny, proves i acceptació final.
		A.14.1.2	Seguretat de les comunicacions en serveis accessibles per xarxes púl	Sí	Garantir la protecció contra activitats fraudulentes, accés, modificació o revelació no autoritzades de la informació que s'utilitza en serveis accessibles per xarxes públiques.
		A.14.1.3	Protecció de les transaccions per xarxes telemàtiques	Sí	Protegir la informació i les transaccions per a prevenir transmissions incompletes o errònies, alteració dels missatges, fuites d'informació no autoritzades o duplicació o reenviament de missatges sense autorització.
	A.14.2 Seguretat en els processos de desenvolupament i suport				
		A.14.2.1	Política de desenvolupament segur dels software	Sí	Definir una política que garanteixi l'ús de les millors pràctiques en el desenvolupament de codi segur.
		A.14.2.2	Procediments de control dels canvis dels sistemes	Sí	Establir procediments que garanteixin que els canvis en el maquinari o programari no comprometin la seguretat del sistema.
		A.14.2.3	Revisió tècnica de les aplicacions després d'haver fet canvis en el sist	Sí	Revisió tècnica de les aplicacions després d'haver fet canvis en el sistema operatiu per a garantir que no hi ha cap afectació sobre la seguretat del sistema.
		A.14.2.4	Restriccions als canvis en els paquets de software	Sí	Les modificacions i canvis en els paquets de programari s'han de limitar al mínim necessari i tots els canvis s'han de realitzar de forma controlada.
		A.14.2.5	Ús de principis d'enginyeria en protecció de sistemes	Sí	Establir els principis d'enginyera segura per a la protecció dels sistemes, documentar-los i aplicar-los sobre tots els sistemes d'informació
		A.14.2.6	Seguretat en entorns de desenvolupament	Sí	Establir les mesures de seguretat de la informació en els entorns no productius.
		A.14.2.7	Externalització del desenvolupament de software	Sí	Supervisió i seguiment de les activitats de desenvolupament de programari externalitzades.
		A.14.2.8	Proves de seguretat durant el desenvolupament dels sistemes	Sí	Realització de proves de seguretat durant el desenvolupament del programari
		A.14.2.9	Proves d'acceptació	Sí	Establir els criteris de seguretat que han d'assolir els nous sistemes d'informació, actualitzacions i noves versions per a ser acceptats i posats en els sistemes productius.
	A.14.3 Dades de prova				
		A.14.3.1	Protecció de les dades utilitzades en les proves	Sí	Les dades per als entorns de proves s'han de seleccionar amb cura, protegir-les i controlar-ne el seu ús.

3.7.11. - A.15 relacions amb subministradors

A.15 RELACIONS AMB SUBMINISTRADORS					
	A.15.1 Seguretat de la informació en les relacions amb els subministradors				
		A.15.1.1	Política de seguretat de la informació amb els subministradors	Sí	Definir la política de seguretat de la informació que han de complir els subministradors que gestionin serveis d'informació o d'actius dels sistemes d'informació corporatius.
		A.15.1.2	Tractament del risc dintre dels acords de subministradors	Sí	S'han d'acordar els requeriments de seguretat de la informació ha de complir amb cada proveïdor que tingui accés, tracti, emmagatzemi o proveeixi components d'infraestructura a l'organització oi documentar-los en un contracte.
		A.15.1.3	Carena de subministrament en tecnologies de la informació i les comu	Sí	Els acords sobre seguretat de la informació han de contemplar el manteniment de la seguretat en el cas que els proveïdors facin una subcontractació dels serveis o bé prohibir-la per contracte.
	A.15.2 Gestió de la prestació del servei pels subministradors				
		A.15.2.1	Supervisió i revisió dels serveis prestats per tercers	Sí	Supervisar i revisar els serveis prestats per tercers a l'organització i si cal reservar el dret a realitzar auditories de compliments dels acords o contractes.
		A.15.2.2	Gestió de canvis en els serveis prestats per tercers	Sí	Els canvis de proveïdors en la provisió de serveis s'ha de realitzar garantint les polítiques i procediments de seguretat que garanteixin la continuïtat de la prestació dels serveis crítics per a l'organització.

3.7.12. - A.16 gestió d'incidents de seguretat de la informació

A.16 GESTIÓ D'INCIDENTS DE SEGURETAT DE LA INFORMACIÓ					
	A.16.1 Gestió d'incidents de seguretat de la informació i millores				
		A.16.1.1	Responsabilitats i procediments	Sí	Establiment de responsabilitats i elaboració de procediments per a assegurar que les incidències de seguretat es gestionen de forma ràpida, efectiva i ordenada per a poder prendre les accions correctives necessàries.
		A.16.1.2	Notificació dels events de seguretat de la informació	Sí	Establir procediments de comunicació a totes les parts implicades dels events de seguretat.
		A.16.1.3	Notificació de punts dèbils de la seguretat	Sí	Els empleats i empreses proveïdores de serveis han de reportar qualsevol debilitat de seguretat que observin en els sistemes d'informació de l'organització
		A.16.1.4	Valoració d'events de seguretat de la informació i presa de decisions	Sí	Els events de seguretat han de ser valorats i s'ha de decidir si es classifiquen com a incidents de seguretat.
		A.16.1.5	Resposta als incidents de seguretat	Sí	S'han d'elaborar procediments per a respondre als incidents de seguretat
		A.16.1.6	Aprenentatge dels incidents de seguretat de la informació	Sí	Utilització del coneixement adquirit en l'anàlisi i resolució d'incidents s'hauria d'utilitzar per a reduir la probabilitat o l'impacte de futurs incidents.
		A.16.1.7	Recopilació d'evidències	Sí	Definició dels procediments per a la identificació, recol·lecció, adquisició i preservació d'informació que pugui ser utilitzada com a evidència.

3.7.13. - A.17 aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci

A.17 ASPECTES DE LA SEGURETAT DE LA INFORMACIÓ EN LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI					
	A.17.1 Continuïtat de la seguretat de la informació				
		A.17.1.1	Planificació de la continuïtat de la seguretat de la informació	Sí	Protegir els processos i activitats crítics del negoci de contingències o desastres, i garantir que es restableix el funcionament normal en uns terminis acceptables des del punt de vista del negoci després d'una situació de desastre.
		A.17.1.2	Implementació de la continuïtat de la seguretat de la informació	Sí	S'establiran, documentaran i implantaran els processos, procediments i controls per a garantir el nivell de la continuïtat de la seguretat de la informació durant situacions adverses.
		A.17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la in	Sí	Es verificaran l'efectivitat i implantació dels controls de continuïtat de la seguretat de la informació de forma periòdica per a garantir que són vàlids i efectius en situacions adverses.
	A.17.2 Redundàncies				
		A.17.2.1	Disponibilitat d'instal·lacions per al processament de la informació	Sí	Les instal·lacions de processament de la informació s'implementaran amb la redundància necessària per a garantir els requeriments de disponibilitat.

3.7.14. - A.18 compliment

A.18 COMPLIMENT					
	A.18.1 Compliment dels requisits legals i contractuals				
		A.18.1.1	Identificació de la legislació aplicable	Sí	Prendre les mesures necessàries per a que totes les obligacions legals, estatutàries, reguladores o contractuals que s'han de complir en matèria de seguretat de la informació són identificades, documentades i mantingudes actualitzades per a donar-los-hi compliment.
		A.18.1.2	Drets de propietat intel·lectual (DPI)	Sí	Implantar els mecanismes per a garantir el compliment amb la legislació i les obligacions legals relacionades amb la propietat intel·lectual.
		A.18.1.3	Protecció dels registres de l'organització	Sí	Cal definir les directrius de la classificació de la informació per a poder definir el seu nivell de protecció segons el seu valor, criticitat i sensibilitat per a l'organització respecte a accessos no autoritzats o la seva revelació.
		A.18.1.4	Protecció de dades i privacitat de la informació de caràcter personal	Sí	Garantir la privacitat i la protecció de les dades de caràcter personal d'acord amb les obligacions legals, estatutàries, reguladores o contractuals aplicables a l'organització.
		A.18.1.5	Regulació dels controls criptogràfics	Sí	Implantar els mecanismes per a garantir el compliment amb la legislació i les obligacions legals dels controls criptogràfics.
	A.18.2 Revisions de la seguretat de la informació				
		A.18.2.1	Revisió independent de la seguretat de la informació	Sí	El sistema de gestió de la seguretat de la informació i la seva implementació s'han de revisar per una entitat independent amb una periodicitat planificada o bé quan s'hagin produït canvis significatius en els SGSI.
		A.18.2.2	Compliment de les polítiques i normes de seguretat	Sí	Els responsables de la informació han de revisar de forma regular els compliment de les polítiques, processos i procediments de la seguretat de la informació que estiguin sota la seva responsabilitat.
		A.18.2.3	Comprovació del compliment	Sí	Els sistemes d'informació han de ser revisats de forma periòdica per garantir el compliment de l'organització amb la política de seguretat i amb els estàndards de referència de la seguretat de la informació.

4. Anàlisi de Riscos

Es realitza una identificació i valoració dels actius, de les amenaces a les que està sotmesa l'organització. Un cop identificats actius i amenaces es realitza una avaluació del risc potencial i del seu impacte.

Es denomina impacte a la mesura del dany sobre l'actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius en vàries dimensions i la degradació que causarien les amenaces es pot derivar l'impacte que aquestes tindrien sobre el sistema.

S'ha seguit la metodologia MAGERIT proposada pel Consell Superior d'Administració Electrònica. S'ha utilitzat l'eina EAR-PILAR del CCN-CERT per a fer l'anàlisi de riscos. Hi ha tres versions de PILAR per a fer l'anàlisi de riscos: PILAR, PILAR-Bàsic i µPILAR.

La realització de l'anàlisi de riscos s'ha fet utilitzant l'eina µPILAR. És l'eina PILAR reduïda a la mínima expressió per la realització d'una anàlisi de riscos molt ràpida. El resultat de l'anàlisi es pot carregar a PILAR per a un estudi més detallat si és vol ampliar en el futur.

La tria de µPILAR a la pràctica no ha permès per a realitzar una anàlisi molt ràpida ja que ha comportat fer la valoració dels perfils corresponents al RD 1720 de protecció de dades de caràcter personal, a la ISO/IEC 27002:2005 i a la ISO/IEC 27002:2013 omplint per a tots ells la valoració de totes les salvaguardes aplicades a totes les amenaces que eren d'aplicació als actius definits. Una tasca que ha comportat més de 16 hores. El resultat ha estat molt complert però no pas ràpid.

Respecte a l'eina µPILAR val a dir que només permet la definició dels actius essencials d'una organització. Això ha fet que no segueixi exactament la classificació proposada a la PAC3 sinó la que ha marcat l'eina.

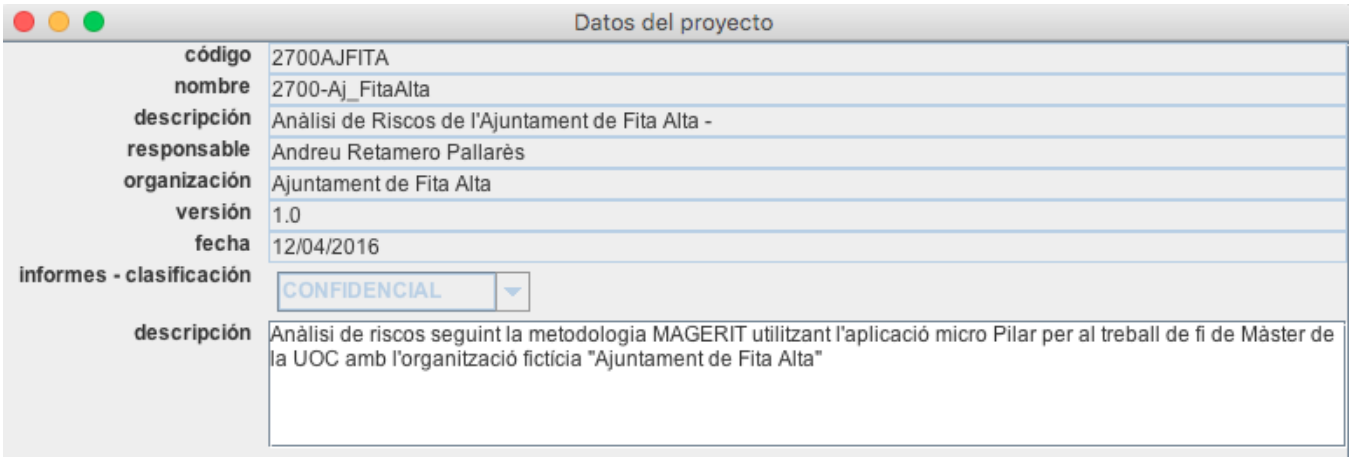
En els diferents apartats s'utilitzarà la informació introduïda a l'eina µPILAR en format de taules sempre que es pugui, o en captures de pantalles o informes de la pròpia eina.

L'anàlisi de riscos s'ha realitzat sobre el domini "Seu Electrònica" el qual correspon al lloc web on l'Ajuntament de Fita Alta té la seva seu electrònica la qual es pot consultar a https://seu.fitaalta.cat . La "Seu electrònica" és un punt d'accés únic a disposició de la ciutadania i de les empreses que representa una nova manera de realitzar les gestions públiques, sense condicionaments horaris ni d'espai, amb la màxima seguretat i contribuint a un ús més eficaç i eficient dels recursos públics. Es configura una oficina virtual oberta a totes hores i tots els dies de l'any.

4.1. Anàlisi dels actius

4.1.1. Dades del projecte

L'eina µPILAR demana unes dades generals del projecte abans de passar a les pantalles de definició d'actius.



4.1.2. Inventari d'actius

La proposta de la metodologia MAGERIT proposa fer una classificació dels actius en diferents classes o àmbits:

- Instal·lacions
- Hardware
- Aplicacions
- Dades
- Xarxa
- Serveis
- Equipament auxiliar
- Personal

L'eina µPILAR no permet aquesta classificació i les restringeix només als actius essencials. S'entenen per actius essencials del sistema:

- la informació que es tracta
- els serveis que es presten
- els punts d'interconnexió amb altres sistemes
- serveis externs (prestats per tercers) en els quals es recolza el sistema

Per a cadascun d'aquests actius, s'indiquen dades administratives, així com la seva valoració (el nivell de seguretat requerit) en termes de **D**isponibilitat, **I**ntegritat, **C**onfidencialitat, **A**utenticitat i **T**raçabilitat.

Activos esenciales

dimensión	[D]	[I]	[C]	[A]	[T]
[2700AJFITA] 2700-Aj_FitaAlta	[1]	[7]	[4]	[7]	[4]
Activos esenciales					
is [INFOPUB] Informació pública	[1]	[4]	[0]	[4]	[0]
is [TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
is [IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
is [CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
is [CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
is [VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4]
is [NOT-ELEC] Notificacions telemàtiques	[1]	[4]	[4]	[4]	[4]
is [LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]
is [POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]
punto de interconexión					
[VLAN-DMZ] VLAN DMZ	[1]	[7]	[4]	[7]	[4]
[Internet] Internet	[1]	[7]	[4]	[7]	[4]
[LINK-REDUNDANT-CPDs] Connexió redundant entre CPDs	[1]	[7]	[4]	[7]	[4]
[VLAN-Servers] VLAN servidors	[1]	[7]	[4]	[7]	[4]
contratado a una tercera parte					
[INET-CORP] Contracte amb Telefònica per accés a internet dels servidors	[1]	[7]	[4]	[7]	[4]
[PSIS] Plataforma de Signatura Electrònica	[1]	[7]	[4]	[7]	[4]
[eTauler] Tauler electrònic AOC	[1]	[7]	[4]	[7]	[4]
[eNotum] Notificacions elctròniques AOC	[1]	[7]	[4]	[7]	[4]
[viaoberta] Serveis d'interoperabilitat AOC	[1]	[7]	[4]	[7]	[4]
[TPV-Virtual] Passarel·la de pagament online	[1]	[7]	[4]	[7]	[4]
[SUB.ELECTRIC] Contracte de subministrament elèctric	[1]	[7]	[4]	[7]	[4]

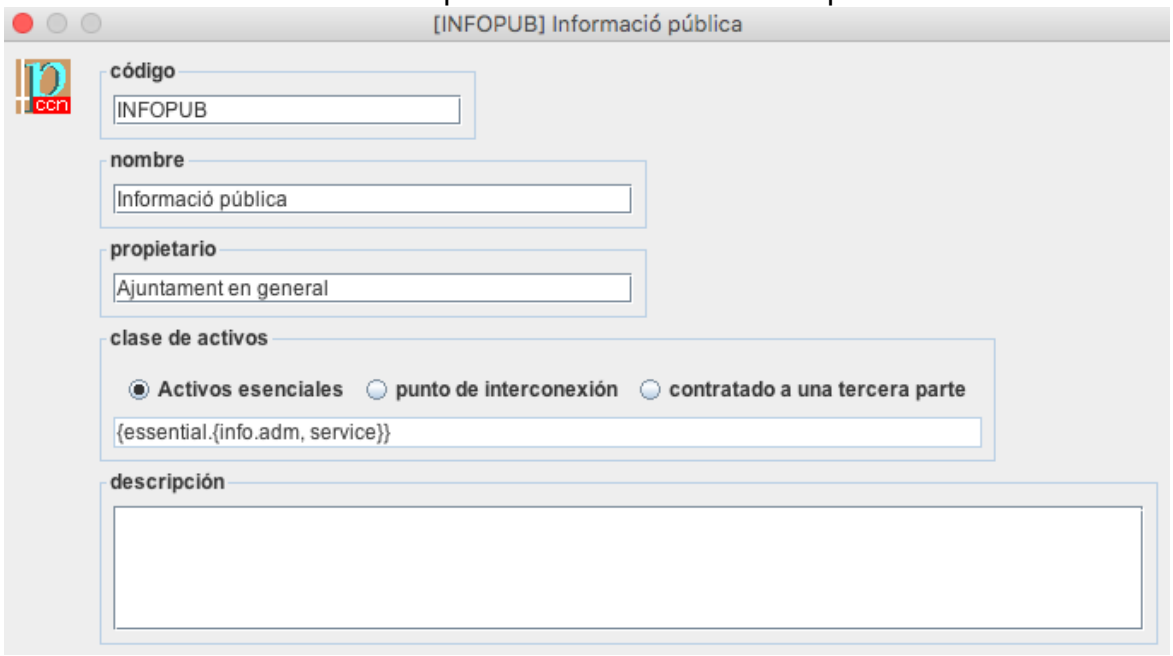
La valoració dels actius s'ha fet d'acord a la taula de nivells següent per a cada nivell de seguretat

10	Nivell 10
9	Nivell 9
8	Nivell 8
7	Alt
6	Nivell 6
5	Nivell 5
4	Mitjà
3	Nivell 3
2	Nivell 2
1	Baix
0	Menyspreable

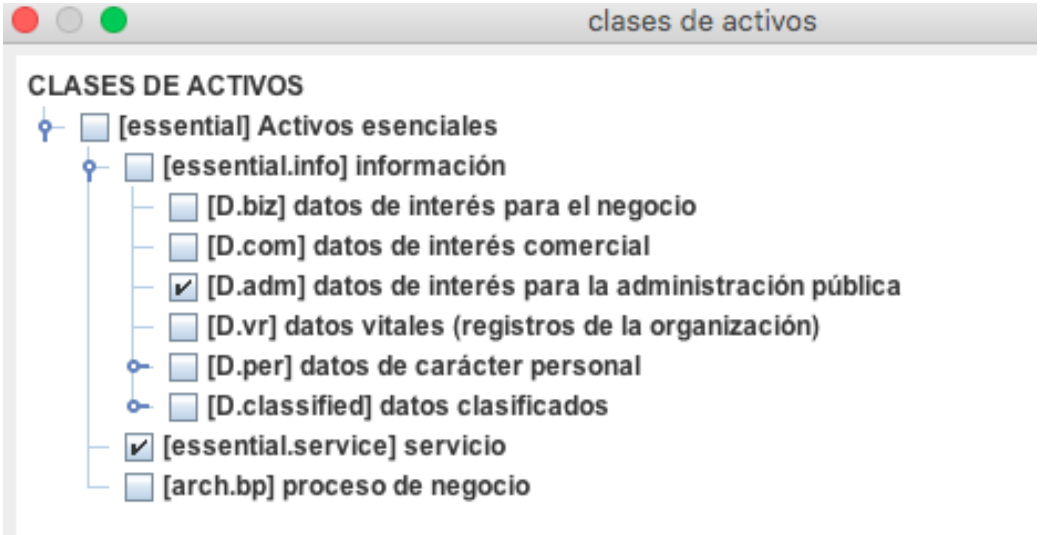
Tots els actius essencials són tant serveis (que s'ofereixen a la ciutadania) com informació (que és la que facilita el servei o bé la que s'emmagatzema com el resultat de la prestació del servei).

- Informació pública
- Tauler d'Edictes Electrònic
- Inici de tràmits
- Carpeta ciutadana
- Carpeta del proveïdor
- Validador de documents
- Notificacions telemàtiques
- Licitacions
- Pagament On-Line

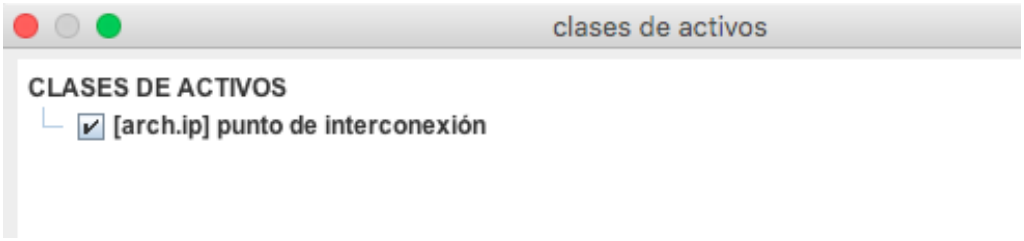
Per a cadascun d'ells s'ha omplert un fitxa on es fa una tipificació addicional.



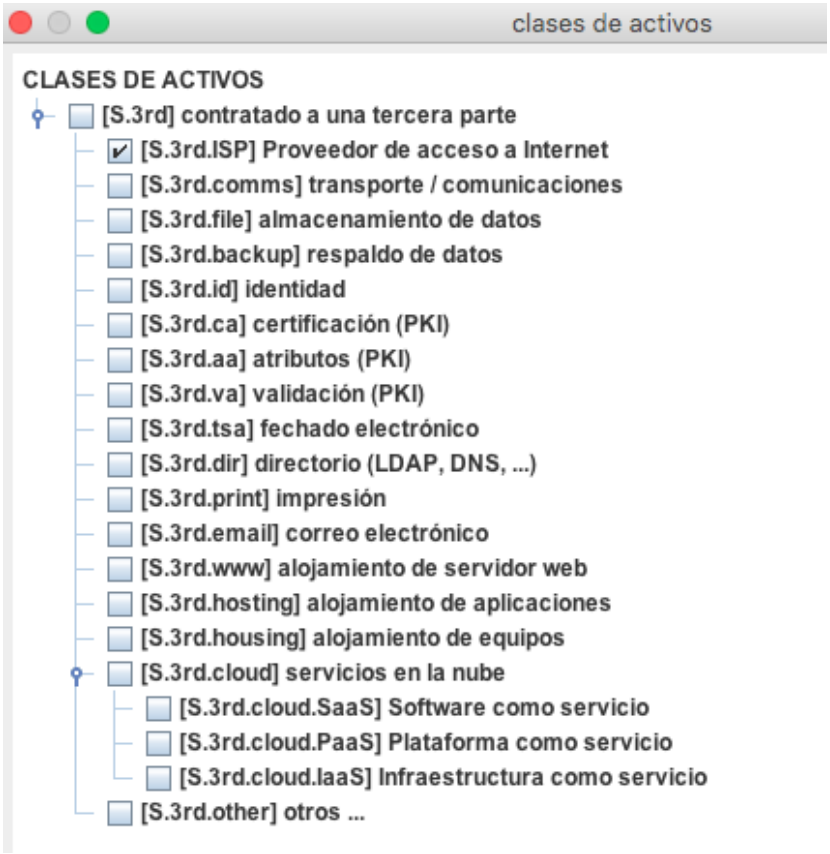
Per als actius essencials



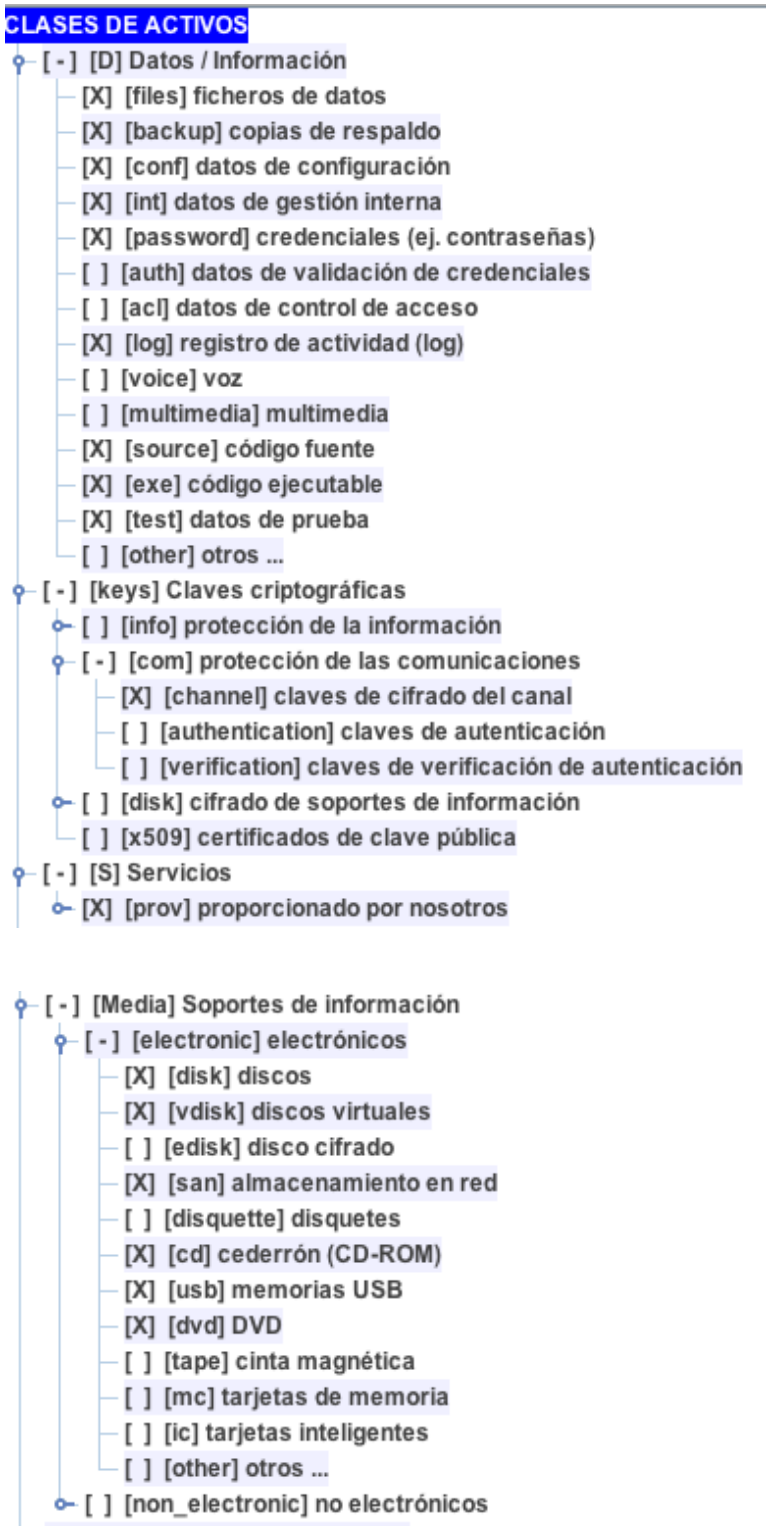
Per als punts d'interconnexió (com la VLAN-DMZ)

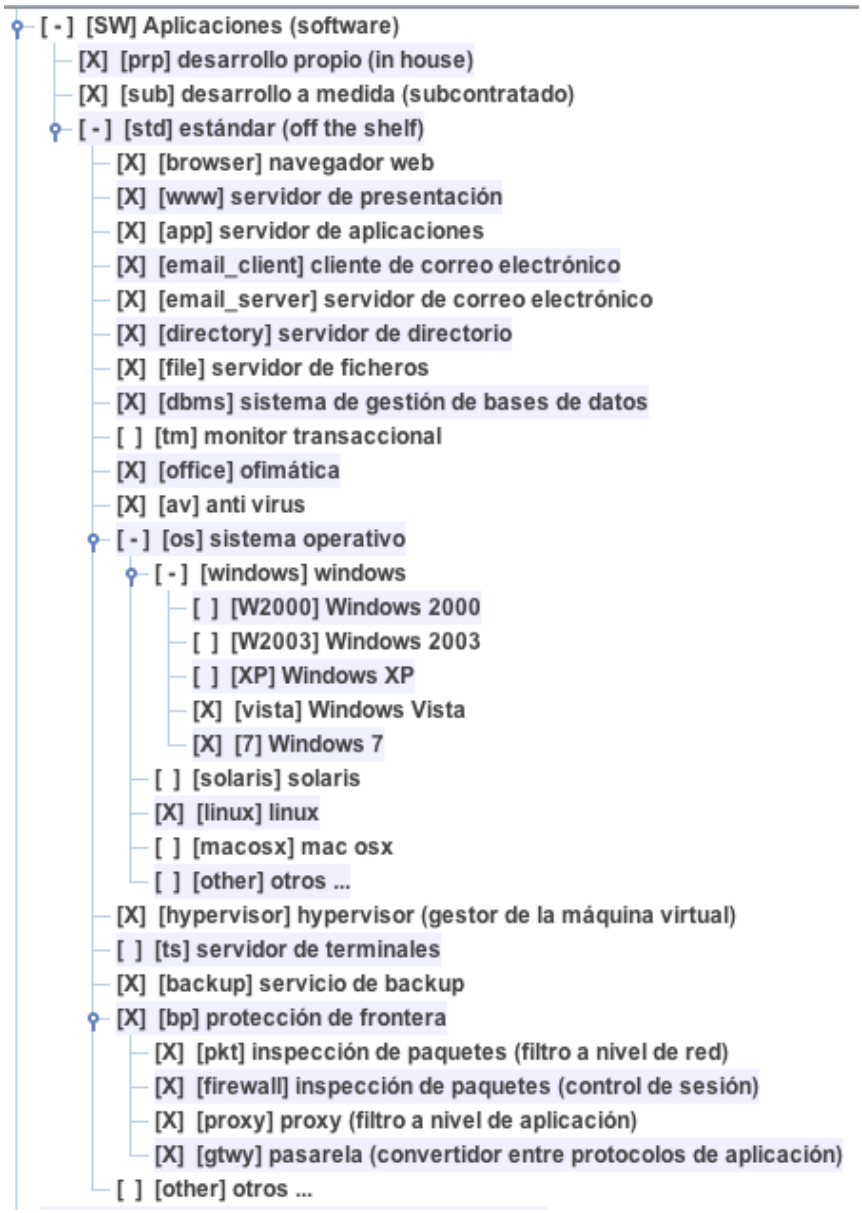


Per als contractats a tercers (com la telefonia per a accedir a internet des dels servidors)



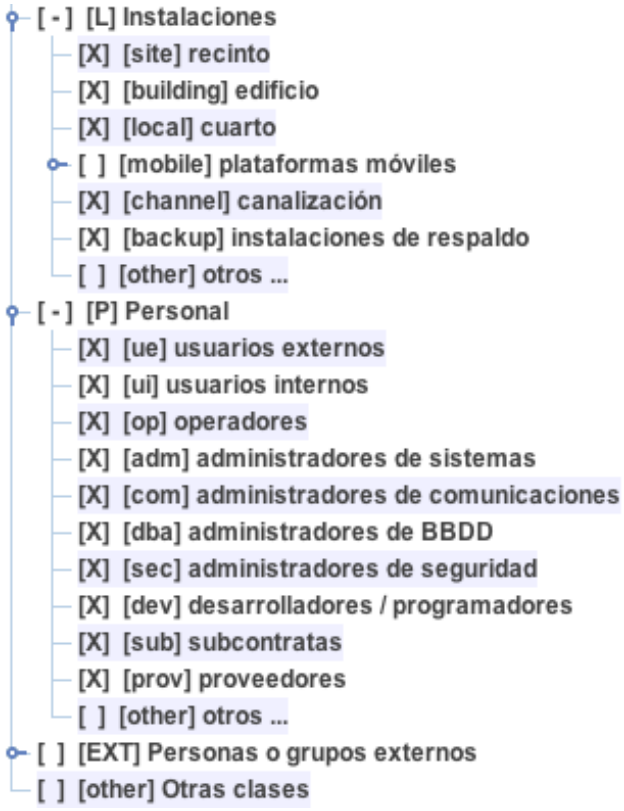
A banda d'una especificació detallada dels actius essencials, μPILAR també demana que s'identifiquin tots els tipus d'actius que hi ha a l'organització sense tenir necessitat de detallar-los. Aquesta especificació serà utilitzada més endavant per a aplicar les amenaces a les que estan exposats els actius i fer l'anàlisi d'amenaces. Relaciono la seqüència de pantalles que reculles aquesta identificació dels tipus d'actius utilitzats.




[-] [SW] Aplicaciones (software)
[X] [prp] desarrollo propio (in house)
[X] [sub] desarrollo a medida (subcontratado)
[-] [std] estándar (off the shelf)
[X] [browser] navegador web
[X] [www] servidor de presentación
[X] [app] servidor de aplicaciones
[X] [email_client] cliente de correo electrónico
[X] [email_server] servidor de correo electrónico
[X] [directory] servidor de directorio
[X] [file] servidor de ficheros
[X] [dbms] sistema de gestión de bases de datos
[ ] [tm] monitor transaccional
[X] [office] ofimática
[X] [av] anti virus
[-] [os] sistema operativo
[-] [windows] windows
[ ] [W2000] Windows 2000
[ ] [W2003] Windows 2003
[ ] [XP] Windows XP
[X] [vista] Windows Vista
[X] [7] Windows 7
[ ] [solaris] solaris
[X] [linux] linux
[ ] [macosx] mac osx
[ ] [other] otros ...
[X] [hypervisor] hypervisor (gestor de la máquina virtual)
[ ] [ts] servidor de terminales
[X] [backup] servicio de backup
[X] [bp] protección de frontera
[X] [pkt] inspección de paquetes (filtro a nivel de red)
[X] [firewall] inspección de paquetes (control de sesión)
[X] [proxy] proxy (filtro a nivel de aplicación)
[X] [gtwy] pasarela (convertidor entre protocolos de aplicación)
[ ] [other] otros ...
[-] [AUX] Equipamiento auxiliar
[X] [power] fuentes de alimentación
[X] [ups] sai - sistemas de alimentación ininterrumpida
[X] [gen] generadores eléctricos
[X] [ac] equipos de climatización
[-] [cabling] cableado de datos
[X] [wire] cable eléctrico
[X] [fiber] fibra óptica
[ ] [supply] suministros esenciales
[X] [destroy] equipos de destrucción de soportes
[X] [furniture] mobiliario
[ ] [safe] cajas fuertes
[ ] [other] otros ...

- [-] [HW] Equipamiento informático (hardware)
  - [X] [host] grandes equipos (host)
  - [ ] [mid] equipos medios
  - [X] [pc] informática personal
  - [X] [mobile] informática móvil
  - [ ] [pda] agendas electrónicas
  - [X] [vhost] equipos virtuales (máquinas virtuales)
  - [X] [cluster] cluster
  - [X] [backup] equipamiento de respaldo
  - [X] [data] que almacena datos
  - [-] [peripheral] periféricos
    - [X] [print] medios de impresión
    - [X] [scan] escáner
    - [ ] [crypto] dispositivo criptográfico
    - [ ] [other] otros ...
  - [-] [robot] robots
    - [ ] [tape] ... de cintas
    - [X] [disk] ... de discos
  - [-] [network] soporte de la red
    - [ ] [modem] módem
    - [ ] [hub] concentrador
    - [X] [switch] conmutador
    - [X] [router] encaminador
    - [ ] [bridge] puente
    - [X] [wap] punto de acceso wireless
    - [ ] [other] otros ...
  - [ ] [pabx] centralita telefónica
  - [ ] [ipphone] teléfono IP
  - [ ] [other] otros ...

- [-] [COM] Redes de comunicaciones
  - [ ] [PSTN] red telefónica
  - [ ] [ISDN] RDSI (red digital)
  - [ ] [X25] X25 (red de datos)
  - [ ] [ADSL] ADSL
  - [ ] [pp] punto a punto
  - [ ] [radio] red inalámbrica
  - [X] [wifi] WiFi
  - [ ] [mobile] telefonía móvil
  - [ ] [sat] por satélite
  - [X] [LAN] red local
  - [X] [VLAN] LAN virtual
  - [ ] [MAN] red metropolitana
  - [ ] [WAN] red de área amplia
  - [X] [Internet] Internet
  - [ ] [vpn] red privada virtual
  - [ ] [backup] comunicaciones de respaldo
  - [ ] [other] otros ...


[-] [L] Instalaciones
[X] [site] recinto
[X] [building] edificio
[X] [local] cuarto
[ ] [mobile] plataformas móviles
[X] [channel] canalización
[X] [backup] instalaciones de respaldo
[ ] [other] otros ...
[-] [P] Personal
[X] [ue] usuarios externos
[X] [ui] usuarios internos
[X] [op] operadores
[X] [adm] administradores de sistemas
[X] [com] administradores de comunicaciones
[X] [dba] administradores de BBDD
[X] [sec] administradores de seguridad
[X] [dev] desarrolladores / programadores
[X] [sub] subcontratas
[X] [prov] proveedores
[ ] [other] otros ...
[ ] [EXT] Personas o grupos externos
[ ] [other] Otras clases

4.1.3. Valoració d'actius

L'eina µPILAR, a diferència de les eines PILAR i PILAR-Basic, només permet fer una anàlisi qualitativa i no permet fer una valoració dels actius. Així que no s'ha pogut realitzar una valoració dels actius seguint la recomanació de MAGERIT i suggerida per a a PAC3 que reculli el valor de l'actiu degut a que l'eina no ho permet.

Els criteris per a la valoració proposats per a cada actiu eren:

- Molt alt
- Alt
- Mig
- Baix
- Molt baix

Aquests criteris també es podien complementar amb una estimació econòmica quantitativa.

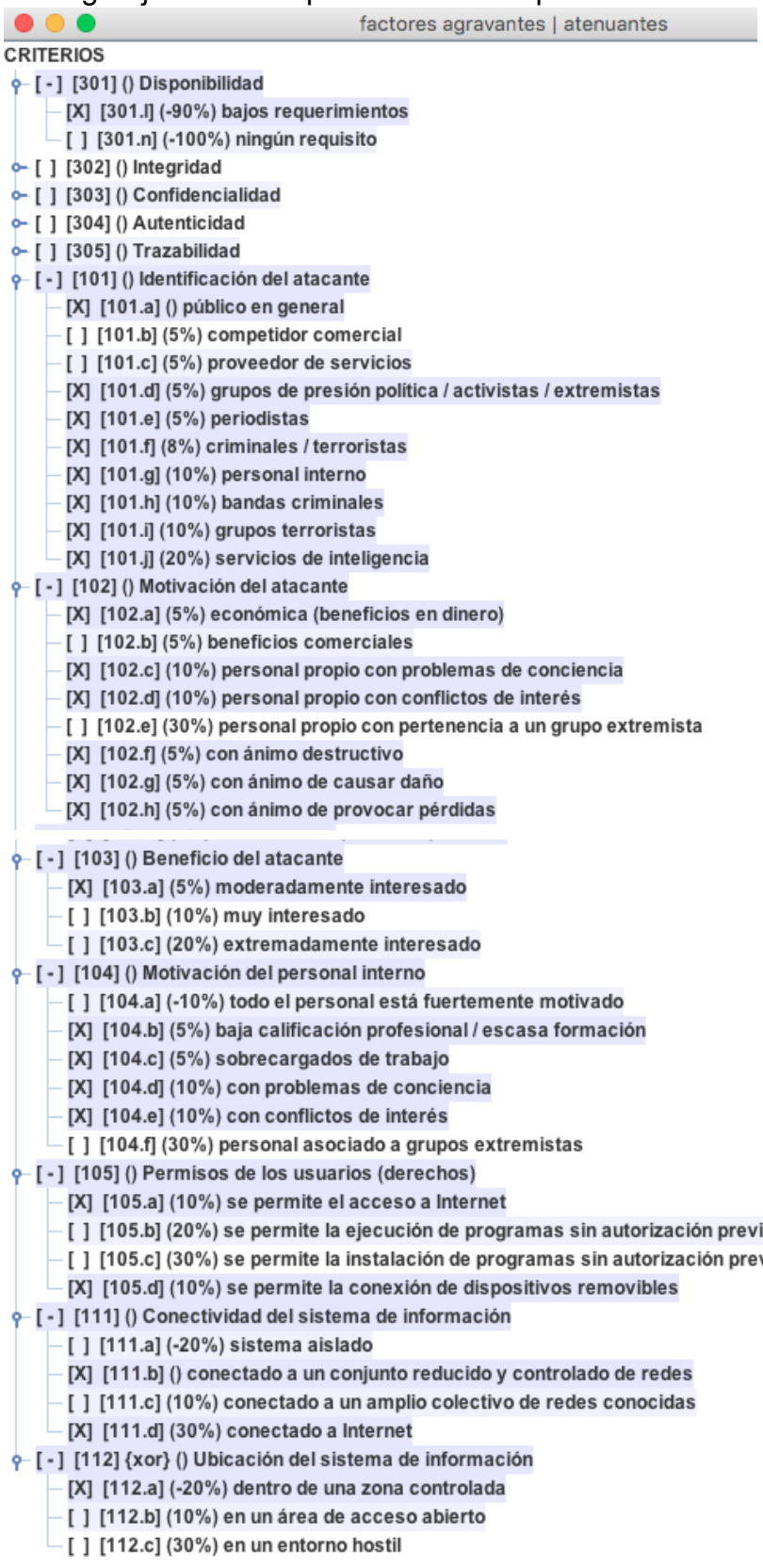
Es torna a adjuntar la valoració dels actius, sense valor econòmic, que realitza l'eina.

Activos esenciales

dimensión	[D]	[I]	[C]	[A]	[T]
[2700AJFITA] 2700-Aj_FitaAlta	[1]	[7]	[4]	[7]	[4]
Activos esenciales					
is [INFOPUB] Informació pública	[1]	[4]	[0]	[4]	[0]
is [TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
is [IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
is [CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
is [CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
is [VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4]
is [NOT-ELEC] Notificacions telemàtiques	[1]	[4]	[4]	[4]	[4]
is [LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]
is [POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]
punto de interconexión					
[VLAN-DMZ] VLAN DMZ	[1]	[7]	[4]	[7]	[4]
[Internet] Internet	[1]	[7]	[4]	[7]	[4]
[LINK-REDUNDANT-CPDs] Connexió redundant entre CPDs	[1]	[7]	[4]	[7]	[4]
[VLAN-Servers] VLAN servidors	[1]	[7]	[4]	[7]	[4]
contratado a una tercera parte					
[INET-CORP] Contracte amb Telefònica per accés a internet dels servidors	[1]	[7]	[4]	[7]	[4]
[PSIS] Plataforma de Signatura Electrònica	[1]	[7]	[4]	[7]	[4]
[eTauler] Tauler electrònic AOC	[1]	[7]	[4]	[7]	[4]
[eNotum] Notificacions elctròniques AOC	[1]	[7]	[4]	[7]	[4]
[viaoberta] Serveis d'interoperabilitat AOC	[1]	[7]	[4]	[7]	[4]
[TPV-Virtual] Passarel·la de pagament online	[1]	[7]	[4]	[7]	[4]
[SUB.ELECTRIC] Contracte de subministrament elèctric	[1]	[7]	[4]	[7]	[4]

4.1.4. Factors agreujants/atenuants

Conjunt de factors que poden ser considerats vulnerabilitats i augmentarien els riscos o l'impacte sobre els actius i d'altres que serien atenuants i el reduirien. Un factor atenuant està marcat amb el signe – per a indicar que disminueix el risc i un factor agreujant no té cap marca i indica que suma.



4.2. Anàlisi d'amenaces

L'eina µPILAR utilitza per a la realització de l'anàlisi de riscos uns perfils de seguretat predefinits els quals utilitza per a associar un conjunt d'amenaces als actius definits segons les seves característiques.

Aquesta associació és precisament un dels avantatges de la utilització de les diferents eines PILAR ja que no cal que ens preocupem de veure quines amenaces són o no són aplicables als actius que hem definit. Les eines PILAR fan aquesta associació basant-se en un recull de les amenaces més comunes basada en el catàleg d'elements punt 2 del llibre II de la metodologia MAGERIT.
Les amenaces estan classificades en els següents grans blocs:

- amenaces d'origen natural
- amenaces de l'entorn (d'origen industrial)
- defectes de les aplicacions
- causades per les persones de forma accidental (errors i fallides no intencionades)
- causades per les persones de forma deliverada (atacs intencionats)

La utilització de l'eina µPILAR fa que no calgui mesurar la degradació que l'amenaça pot provocar sobre l'actiu ni la probabilitat que aquesta amenaça es materialitzi. Totes aquestes funcions es realitzen de forma automàtica basant-se en dades històriques acumulades i que permeten fer de forma automàtica la determinació de l'impacte potencial.

Els perfils de seguretat que s'han utilitzat per a l'avaluació del domini "Seu electrònica" han estat:

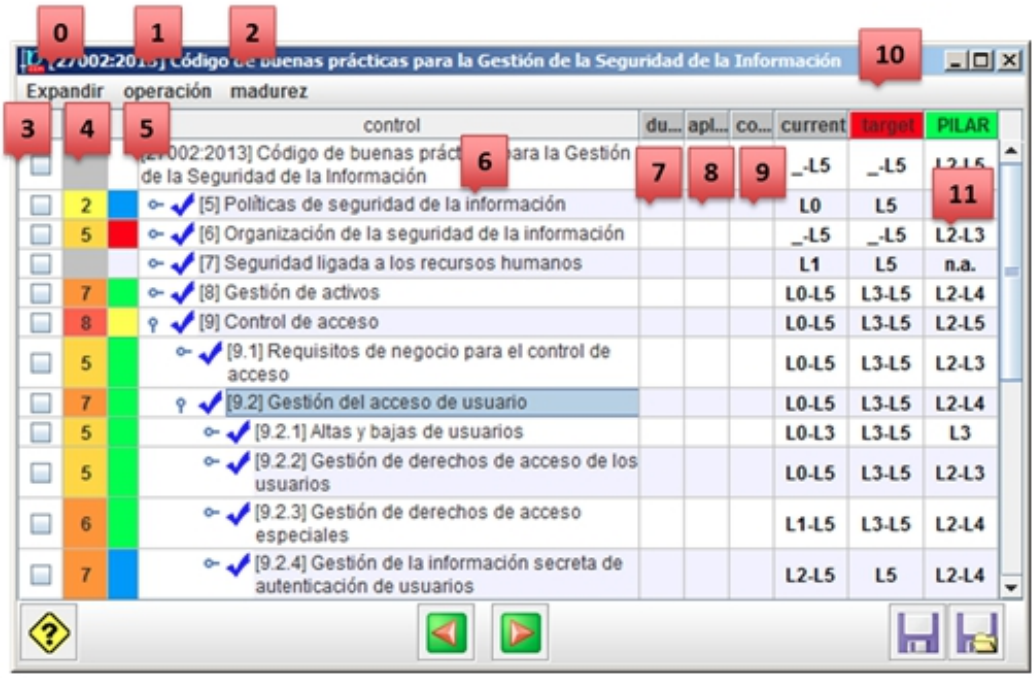
- RD 1720 de protecció de dades de caràcter personal
- ISO/IEC 27002:2005
- ISO/IEC 27002:2013

S'han utilitzat tots els perfils de seguretat que proposava l'eina µPILAR ja que són d'aplicació per a una administració pública espanyols. L'eina utilitza els dos perfils de la ISO/IEC 27002 (el de 2005 i el de 2013) però no permet seleccionar només un d'ells sinó que els presenta tots dos.

Per a tots ells s'ha fet la valoració de totes les salvaguardes aplicades a totes les amenaces que eren d'aplicació als actius definits. Una tasca que ha comportat més de 16 hores. El resultat ha estat molt complert però no pas ràpid.

4.2.1. Avaluació dels perfils de seguretat

Aquesta avaluació presenta el compliment d'un determinat perfil de seguretat amb l'objectiu d'assolir un objectiu final (anomenat PILAR) passant per una fase intermèdia (anomenada objectiu i a la qual se li hauria de fixar un termini) i partint de l'estat actual.



Es marquen les parts més significatives traient la informació del manual de l'eina. A la captura anterior i en l'exercici realitzat es mostren les dades en el format de nivells de maduresa (de L1 a L5).

2	porcentaje	En [11] PILAR presenta: **porcentaje** — porcentaje de cumplimiento de los controles — madurez de las salvaguardas **madurez** — madurez de controles y salvaguardas **cobertura de PILAR** — porcentaje de cumplimiento de la recomendación de PILAR; es decir, 100% significa que la madurez es igual o superior a la recomendada por PILAR

4	recomendación	Un valor en el rango [null .. 10] estimado por PILAR teniendo en cuenta los activos declarados, la valoración en cada dimensión de seguridad y el nivel de riesgo afrontado por esta medida o control. La celda queda gris (null) si PILAR no encuentra ninguna razón para recomendar la medida. (o) - PILAR piensa que es excesivo ("overkill"). (u) - PILAR piensa que es insuficiente ("underkill").
5	traffic light	Compra la valoración en la fase de referencia (ROJA) con la valoración en la fase objetivo (VERDE) y muestra un color: ROJO el valor en la fase de referencia es muy inferior al del objetivo AMARILLO el valor en la fase de referencia es inferior al del objetivo VERDE el valor en la fase de referencia es igual al del objetivo AZUL el valor en la fase de referencia es superior al del objetivo Ver "*Fases de referencia y objetivo*".
6		Árbol de controles Presenta los controles que componen el perfil en forma de árbol jerárquico. Cuando terminan los controles formales, PILAR sigue desplegando las salvaguardas asociadas a ellos, o preguntas específicas. Haga clic para expandir / colapsar una rama del árbol. Haga clic con el botón derecho para acceder a "*EVL / tree*".

10	fases	Fses del proyecto. Haga clic con el botón izquierdo para seleccionar la fase de referencia (ROJA). Haga clic con el botón derecho para seleccionar la fase objetivo (VERDE). Ver "*Fases de referencia y objetivo*".
11		Ver "*EVL / Valuation*

Donarem també les indicacions que ens proporciona l'eina per a interpretar les valoracions del perfil.

Valoración del perfil

[SC] System and Communications Protection				29%	58%	96%
[SC-1] System and Communications Protection Policy and Procedures				24%	79%	95%
[SC-2] Application Partitioning				50%	45%	98%
[H142] There are separate accounts for security administration				L0	L0	L5
[H287] Administration and operation responsibilities are separated				L5	L3	L4
[H244] Establishment of specific menus to control access to the applications' functions		n.a.				

Para los controles y salvaguardas que son de aplicación, puede indicar una valoración en cada fase del proyecto. La valoración se aplica a las hojas terminales del árbol; si aplica una valoración a un nodo con ramas, el valor se propaga hasta las hojas.

El valor que se muestra en los nodos intermedios depende de la selección en [2].

porcentaje PILAR estima un porcentaje de cumplimiento derivado de los niveles de madurez de las ramas.

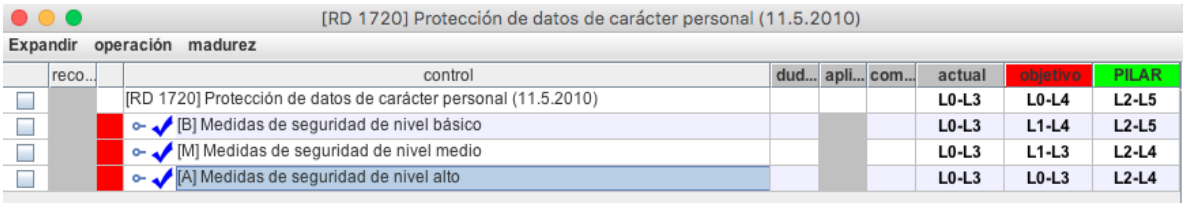
madurez PILAR presenta el rango de madurez de las ramas.

PILAR PILAR compara la madurez en la fase correspondiente con la madurez de la columna PILAR. Si la madurez es igual o superior, PILAR dice que el cumplimiento es del 100%. Si es inferior, el porcentaje disminuye.

Donades les indicacions per a poder interpretar les avaluacions dels perfils de seguretat passarem a detallar-les una per una.

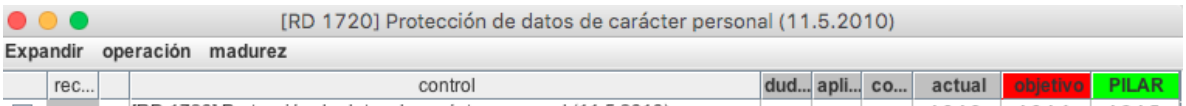
4.2.2. RD 1720 de protecció de dades de caràcter personal

Es mostren les pantalles d'avaluació del perfil de protecció de dades de caràcter personal.



	reco...		control	dud...	apli...	com...	actual	objetivo	PILAR
☐			[RD 1720] Protección de datos de carácter personal (11.5.2010)				L0-L3	L0-L4	L2-L5
☐			[B] Medidas de seguridad de nivel básico				L0-L3	L1-L4	L2-L5
☐			[M] Medidas de seguridad de nivel medio				L0-L3	L1-L3	L2-L4
☐			[A] Medidas de seguridad de nivel alto				L0-L3	L0-L3	L2-L4

El detall a nivell de controls per a cada mesura de seguretat del RD 1720



	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
☐			[RD 1720] Protección de datos de carácter personal (11.5.2010)				L0-L3	L0-L4	L2-L5
☐			[B] Medidas de seguridad de nivel básico				L0-L3	L1-L4	L2-L5
☐			[89] Funciones y obligaciones del personal				L1-L3	L2-L3	L2-L3
☐			[89.1] funciones y obligaciones de los usuarios				L1-L3	L2-L3	L2-L3
☐			[89.2] el personal conoce las normas de seguridad				L1-L2	L2-L3	L2
☐			[90] Gestión de las incidencias				L2-L3	L3	L3
☐			[91] Control de acceso				L0-L2	L1-L3	L2-L5
☐			[91.1] acceso limitado de los usuarios				L0-L2	L1-L3	L3
☐			[91.2] relación de usuarios y privilegios				L0-L2	L1-L3	L2-L3
☐			[91.3] control de acceso				L0-L2	L2-L3	L4-L5
☐			[91.4] control del control de acceso				L0	L1	L3
☐			[91.5] acceso de personal ajeno				L2	L2	n.a.
☐			[92] Gestión de soportes y documentos				L0-L2	L1-L2	L2-L3
☐			[92.1] etiquetado y control de acceso				L0	L2	L3
☐			[92.2] salida de soportes				L0	L2	L2-L3
☐			[92.3] protección durante el transporte				L0	L2	L2-L3
☐			[92.4] destrucción o borrado				L0-L2	L2	L2-L3
☐			[92.5] etiquetado				L0	L1	n.a.
☐			[93] Identificación y autenticación				L2-L3	L3-L4	L3-L4
☐			[93.1] medidas de identificación y autenticación				L2	L4	L3-L4
☐			[93.2] identificación singular				L2-L3	L3	L3
☐			[93.3] uso de contraseñas				n.a.	n.a.	n.a.
☐			[93.4] cambio regular de contraseñas				L3	L3	n.a.
☐			[94] Copias de respaldo y recuperación				L0-L3	L1-L3	L3
☐			[94.1] realización de copias de respaldo				L0-L3	L2-L3	L3
☐			[94.2] recuperación de datos				L2	L3	L3
☐			[94.3] revisión periódica de los procedimientos				L0	L2	L3
☐			[94.4] datos para pruebas				L0-L3	L1-L3	L3
☐			[M] Medidas de seguridad de nivel medio				L0-L3	L1-L3	L2-L4
☐			[A] Medidas de seguridad de nivel alto				L0-L3	L0-L3	L2-L4

[RD 1720] Protección de datos de carácter personal (11.5.2010)

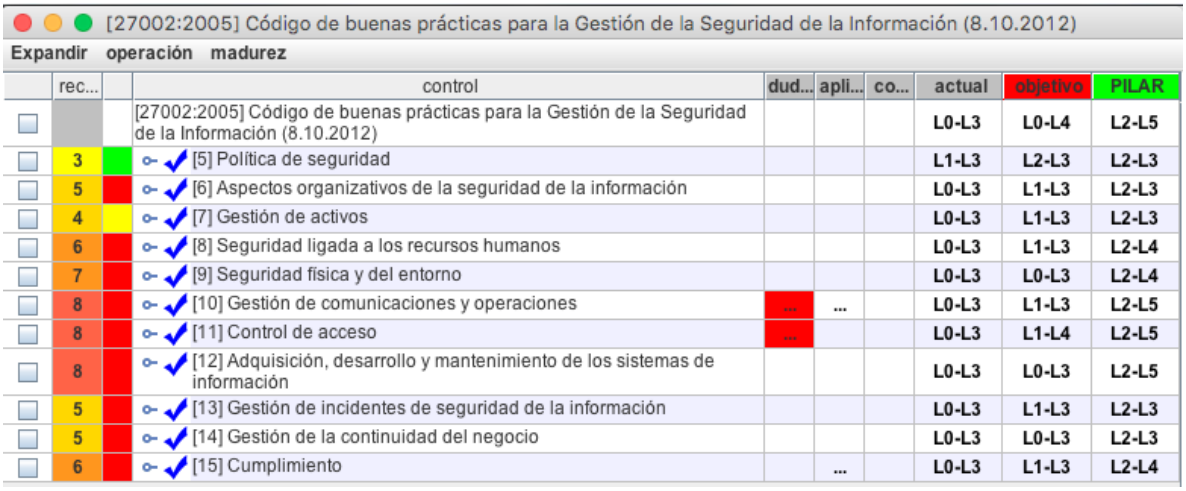
Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
☐			[RD 1720] Protección de datos de carácter personal (11.5.2010)				L0-L3	L0-L4	L2-L5
☐			[B] Medidas de seguridad de nivel básico				L0-L3	L1-L4	L2-L5
☐			[M] Medidas de seguridad de nivel medio				L0-L3	L1-L3	L2-L4
☐			[95] Responsable de seguridad				L3	L3	n.a.
☐			[96] Auditoría				L2	L2	L2
☐			[96.1] auditoría periódica				L2	L2	L2
☐			[96.2] informe de auditoría				L2	L2	n.a.
☐			[96.3] gestión del informe de auditoría				L2	L2	n.a.
☐			[97] Gestión de soportes y documentos				L0	L2	L2-L3
☐			[97.1] registro de entrada de soportes				L0	L2	L2-L3
☐			[97.2] registro de salida				L0	L2	L2-L3
☐			[98] Identificación y autenticación				L0-L3	L2-L3	L3
☐			[99] Control de acceso físico				L0-L3	L1-L3	L2-L4
☐			[100] Registro de incidencias				L1-L3	L2-L3	L3
☐			[100.1] registro de recuperación de datos				L3	L3	n.a.
☐			[100.2] autorización para la recuperación de datos				L1-L2	L2-L3	L3
☐			[A] Medidas de seguridad de nivel alto				L0-L3	L0-L3	L2-L4
☐			[101] Gestión y distribución de soportes				L0-L2	L0-L3	L2-L4
☐			[101.1] etiquetado de los soportes				L0	L0-L2	L3
☐			[101.2] cifrado de los soportes				L0-L2	L1-L3	L2-L4
☐			[101.3] tratamiento en entornos desprotegidos				L1	L2	L2
☐			[102] Copias de respaldo y recuperación				L1-L3	L2-L3	L3
☐			[103] Registro de accesos				L0-L3	L0-L3	L2-L3
☐			[103.1] elementos registrados				L0-L1	L0-L2	L2
☐			[103.2] accesos autorizados				L0	L0	n.a.
☐			[103.3] protección de los registros				L0-L3	L2-L3	L3
☐			[103.4] retención de los registros				L0	L0-L2	L2
☐			[103.5] revisión de los registros				L0-L3	L0-L3	L3
☐			[103.6] exención de la obligación de registrar				L0-L3	L0-L3	n.a.
☐			[104] Telecomunicaciones				L1-L2	L2-L3	L3

A l'aplicació s'ha detallat a nivell de preguntes i de salvaguardes però no es veu reflectit a les figures que es mostren ja que llavors es perdria la visió de conjunt.

4.2.3. ISO/IEC 27002:2005

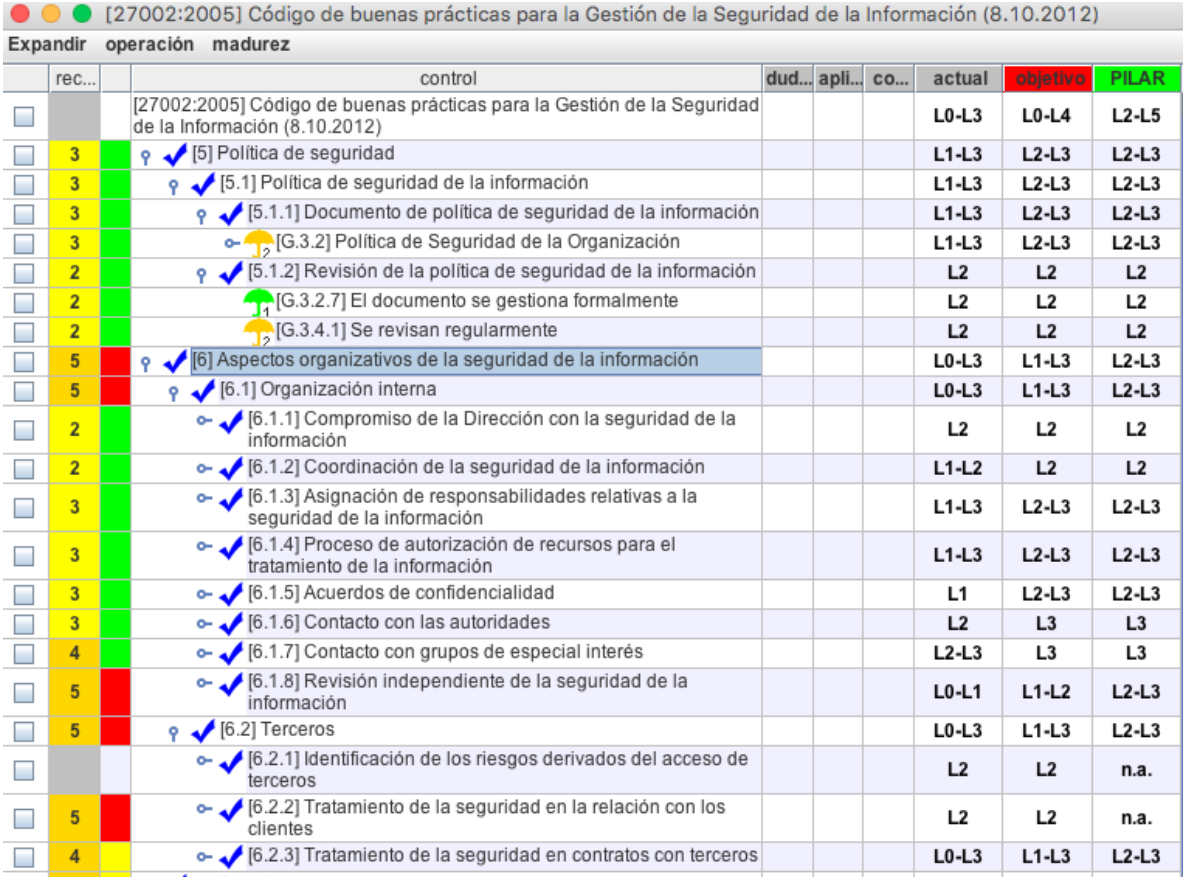
Es mostren les pantalles d'avaluació del perfil de la ISO/IEC 27002:2005



[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
			[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)				L0-L3	L0-L4	L2-L5
	3		[5] Política de seguridad				L1-L3	L2-L3	L2-L3
	5		[6] Aspectos organizativos de la seguridad de la información				L0-L3	L1-L3	L2-L3
	4		[7] Gestión de activos				L0-L3	L1-L3	L2-L3
	6		[8] Seguridad ligada a los recursos humanos				L0-L3	L1-L3	L2-L4
	7		[9] Seguridad física y del entorno				L0-L3	L0-L3	L2-L4
	8		[10] Gestión de comunicaciones y operaciones	...	...		L0-L3	L1-L3	L2-L5
	8		[11] Control de acceso	...			L0-L3	L1-L4	L2-L5
	8		[12] Adquisición, desarrollo y mantenimiento de los sistemas de información				L0-L3	L0-L3	L2-L5
	5		[13] Gestión de incidentes de seguridad de la información				L0-L3	L1-L3	L2-L3
	5		[14] Gestión de la continuidad del negocio				L0-L3	L0-L3	L2-L3
	6		[15] Cumplimiento		...		L0-L3	L1-L3	L2-L4



[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
			[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)				L0-L3	L0-L4	L2-L5
	3		[5] Política de seguridad				L1-L3	L2-L3	L2-L3
	3		[5.1] Política de seguridad de la información				L1-L3	L2-L3	L2-L3
	3		[5.1.1] Documento de política de seguridad de la información				L1-L3	L2-L3	L2-L3
	3		[G.3.2] Política de Seguridad de la Organización				L1-L3	L2-L3	L2-L3
	2		[5.1.2] Revisión de la política de seguridad de la información				L2	L2	L2
	2		[G.3.2.7] El documento se gestiona formalmente				L2	L2	L2
	2		[G.3.4.1] Se revisan regularmente				L2	L2	L2
	5		[6] Aspectos organizativos de la seguridad de la información				L0-L3	L1-L3	L2-L3
	5		[6.1] Organización interna				L0-L3	L1-L3	L2-L3
	2		[6.1.1] Compromiso de la Dirección con la seguridad de la información				L2	L2	L2
	2		[6.1.2] Coordinación de la seguridad de la información				L1-L2	L2	L2
	3		[6.1.3] Asignación de responsabilidades relativas a la seguridad de la información				L1-L3	L2-L3	L2-L3
	3		[6.1.4] Proceso de autorización de recursos para el tratamiento de la información				L1-L3	L2-L3	L2-L3
	3		[6.1.5] Acuerdos de confidencialidad				L1	L2-L3	L2-L3
	3		[6.1.6] Contacto con las autoridades				L2	L3	L3
	4		[6.1.7] Contacto con grupos de especial interés				L2-L3	L3	L3
	5		[6.1.8] Revisión independiente de la seguridad de la información				L0-L1	L1-L2	L2-L3
	5		[6.2] Terceros				L0-L3	L1-L3	L2-L3
			[6.2.1] Identificación de los riesgos derivados del acceso de terceros				L2	L2	n.a.
	5		[6.2.2] Tratamiento de la seguridad en la relación con los clientes				L2	L2	n.a.
	4		[6.2.3] Tratamiento de la seguridad en contratos con terceros				L0-L3	L1-L3	L2-L3

[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
			[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)				L0-L3	L0-L4	L2-L5
	3		[5] Política de seguridad				L1-L3	L2-L3	L2-L3
	5		[6] Aspectos organizativos de la seguridad de la información				L0-L3	L1-L3	L2-L3
	4		[7] Gestión de activos				L0-L3	L1-L3	L2-L3
	4		[7.1] Responsabilidad sobre los activos				L0-L3	L1-L3	L2-L3
	4		[7.1.1] Inventario de activos				L0-L3	L1-L3	L2-L3
	3		[7.1.2] Propiedad de los activos				L0-L2	L1-L3	L2-L3
	3		[7.1.3] Uso aceptable de los activos				L0-L3	L1-L3	L2-L3
	3		[7.2] Clasificación de la información				L0-L2	L2	L2-L3
	3		[7.2.1] Directrices de clasificación				L0-L2	L2	L2-L3
	3		[7.2.2] Etiquetado y manipulado de la información				L0	L2	L3
	6		[8] Seguridad ligada a los recursos humanos				L0-L3	L1-L3	L2-L4
	4		[8.1] Antes del empleo				L0-L3	L1-L3	L2-L3
	3		[8.1.1] Funciones y responsabilidades				L0-L2	L1-L2	L2-L3
	4		[8.1.2] Investigación de antecedentes				L0-L1	L1-L2	L3
	3		[8.1.3] Términos y condiciones de contratación				L1-L3	L2-L3	L2-L3
	6		[8.2] Durante el empleo				L0-L3	L1-L3	L2-L4
	3		[8.2.1] Responsabilidades de la Dirección				L0-L2	L2-L3	L2-L3
	6		[8.2.2] Concienciación, formación y capacitación en seguridad de la información				L0-L2	L1-L2	L2-L4
	3		[8.2.3] Proceso disciplinario				L1-L3	L2-L3	L2-L3
	5		[8.3] Cese del empleo o cambio de puesto de trabajo				L0-L2	L1-L3	L2-L3
	3		[8.3.1] Responsabilidad del cese o cambio				L0-L1	L1-L2	L2-L3
	5		[8.3.2] Devolución de activos				L2	L3	L3
	5		[8.3.3] Retirada de los derechos de acceso				L2	L3	L3

[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
			[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)				L0-L3	L0-L4	L2-L5
	3		[5] Política de seguridad				L1-L3	L2-L3	L2-L3
	5		[6] Aspectos organizativos de la seguridad de la información				L0-L3	L1-L3	L2-L3
	4		[7] Gestión de activos				L0-L3	L1-L3	L2-L3
	6		[8] Seguridad ligada a los recursos humanos				L0-L3	L1-L3	L2-L4
	7		[9] Seguridad física y del entorno				L0-L3	L0-L3	L2-L4
	7		[9.1] Áreas seguras				L0-L3	L1-L3	L2-L4
	5		[9.1.1] Perímetro de seguridad física				L1-L2	L2-L3	L3
	7		[9.1.2] Controles físicos de entrada				L0-L3	L1-L3	L2-L4
	7		[9.1.3] Seguridad de oficinas, despachos e instalaciones				L0-L3	L1-L3	L3-L4
	6		[9.1.4] Protección contra las amenazas externas y de origen ambiental				L0-L3	L1-L3	L2-L4
	5		[9.1.5] Trabajo en áreas seguras				L0-L3	L1-L3	L2-L3
	5		[9.1.6] Áreas de acceso público y de carga y descarga				L1-L3	L2-L3	L3
	6		[9.2] Seguridad de los equipos				L0-L3	L0-L3	L2-L4
	5		[9.2.1] Emplazamiento y protección de equipos				L0-L3	L2-L3	L2-L3
	5		[9.2.2] Instalaciones de suministro				L0-L3	L0-L3	L2-L3
	6		[9.2.3] Seguridad del cableado				L1-L3	L2-L3	L2-L4
	4		[9.2.4] Mantenimiento de los equipos				L0-L3	L1-L3	L2-L3
	4		[9.2.5] Seguridad de los equipos fuera de las instalaciones				L0	L1-L2	L2-L3
	4		[9.2.6] Reutilización o retirada segura de equipos				L0-L2	L2	L2-L3
	4		[9.2.7] Retirada de materiales propiedad de la empresa				L0	L1-L2	L2-L3
	8		[10] Gestión de comunicaciones y operaciones	...	...		L0-L3	L1-L3	L2-L5
	5		[10.1] Responsabilidades y procedimientos de operación				L0-L3	L1-L3	L2-L3
	6		[10.2] Gestión de la provisión de servicios por terceros				L0-L3	L1-L3	L2-L4
	4		[10.3] Planificación y aceptación del sistema				L0-L2	L1-L3	L2-L3
	7		[10.4] Protección contra el código malicioso y descargable				L0-L3	L2-L3	L2-L4
	5		[10.5] Copias de seguridad				L0-L3	L2-L3	L2-L3
	8		[10.6] Gestión de la seguridad de las redes	...			L0-L3	L2-L3	L2-L5
	5		[10.7] Manipulación de los soportes				L0-L3	L2-L3	L2-L3
	6		[10.8] Intercambio de información				L0-L3	L1-L3	L2-L4
	6		[10.9] Servicios de comercio electrónico		...		L2	L2-L3	L2-L3
	6		[10.10] Supervisión				L0-L3	L1-L3	L2-L4

[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
☐	8		[11] Control de acceso	...			L0-L3	L1-L4	L2-L5
☐	5		[11.1] Requisitos de negocio para el control de acceso				L0-L3	L1-L3	L2-L3
☐	5		[11.1.1] Política de control de acceso				L0-L3	L1-L3	L2-L3
☐	8		[11.2] Gestión de acceso de usuario				L0-L3	L1-L3	L2-L5
☐	5		[11.2.1] Registro de usuario				L0-L3	L2-L3	L2-L3
☐	5		[11.2.2] Gestión de privilegios				L0-L2	L1-L3	L2-L3
☐	8		[11.2.3] Gestión de contraseñas de usuario				L0-L3	L2-L3	L2-L5
☐	5		[11.2.4] Revisión de derechos de acceso de usuario				L0-L2	L2-L3	L3
☐	8		[11.3] Responsabilidades de usuario				L0-L3	L2-L4	L3-L5
☐	7		[11.3.1] Uso de contraseñas				L2	L4	L4
☐	8		[11.3.2] Equipo de usuario desatendido				L1-L3	L2-L3	L3-L5
☐	5		[11.3.3] Política de puesto de trabajo despejado y pantalla limpia				L0-L2	L2-L3	L3
☐	6		[11.4] Control de acceso a la red	...			L1-L3	L2-L3	L2-L4
☐	2		[11.4.1] Política de uso de los servicios en red				L1	L2	L2
☐	5		[11.4.2] Autenticación de usuario para conexiones externas				L3	L3	L3
☐	3		[11.4.3] Identificación de los equipos en las redes				L3	L3	L3
☐	4		[11.4.4] Diagnóstico remoto y protección de los puertos de configuración	...			L1	L2	L3
☐	6		[11.4.5] Segregación de las redes				L3	L3	L3-L4
☐	4		[11.4.6] Control de la conexión a la red	...			L1-L3	L2-L3	L2-L3
☐	3		[11.4.7] Control de encaminamiento (routing) de red				L3	L3	L3
☐	8		[11.5] Control de acceso al sistema operativo				L0-L3	L1-L4	L2-L5
☐	6		[11.5.1] Procedimientos seguros de inicio de sesión				L0-L3	L2-L3	L3-L4
☐	7		[11.5.2] Identificación y autenticación de usuario				L0-L3	L2-L4	L2-L4
☐	5		[11.5.3] Sistema de gestión de contraseñas				L3	L3	L3
☐	5		[11.5.4] Uso de los recursos del sistema				L0-L2	L1-L3	L3
☐	8		[11.5.5] Desconexión automática de sesión				L3	L3	L5
☐	5		[11.5.6] Limitación del tiempo de conexión				L0-L3	L2-L3	L3
☐	7		[11.6] Control de acceso a las aplicaciones y a la información				L1-L3	L2-L3	L2-L4
☐	5		[11.6.1] Restricción del acceso a la información				L2	L2-L3	L2-L3
☐	7		[11.6.2] Aislamiento de sistemas sensibles				L1-L3	L3	L3-L4
☐	4		[11.7] Ordenadores portátiles y teletrabajo				L0-L2	L1-L2	L2-L3
☐	3		[11.7.1] Ordenadores portátiles y comunicaciones móviles				L0-L2	L1-L2	L2-L3
☐	4		[11.7.2] Teletrabajo				L0-L2	L1-L2	L2-L3
			[12] Adquisición, desarrollo y mantenimiento de los sistemas de						

[27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información (8.10.2012)

Expandir operación madurez

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
☐	8		[12] Adquisición, desarrollo y mantenimiento de los sistemas de información				L0-L3	L0-L3	L2-L5
☐	3		[12.1] Requisitos de seguridad de los sistemas de información				L0-L2	L2	L2-L3
☐	3		[12.1.1] Análisis y especificación de los requisitos de seguridad				L0-L2	L2	L2-L3
☐	5		[12.2] Tratamiento correcto de las aplicaciones				L0-L1	L1-L2	L2-L3
☐	4		[12.2.1] Validación de los datos de entrada				L0-L1	L2	L2-L3
☐	4		[12.2.2] Control del procesamiento interno				L0-L1	L1-L2	L2-L3
☐	5		[12.2.3] Integridad de los mensajes				L1	L2	L3
☐	3		[12.2.4] Validación de los datos de salida				L0	L1	L2-L3
☐	8		[12.3] Controles criptográficos				L0-L3	L1-L3	L2-L5
☐	2		[12.3.1] Política de uso de los controles criptográficos				L0-L2	L2	L2
☐	8		[12.3.2] Gestión de claves				L0-L3	L1-L3	L2-L5
☐	7		[12.4] Seguridad de los archivos del sistema				L0-L3	L1-L3	L2-L4
☐	7		[12.4.1] Control del software en explotación				L0-L3	L1-L3	L2-L4
☐	4		[12.4.2] Protección de los datos de prueba del sistema				L3	L3	L3
☐	4		[12.4.3] Control de acceso al código fuente de los programas				L0-L2	L1-L3	L2-L3
☐	5		[12.5] Seguridad en los procesos de desarrollo y soporte				L0-L3	L0-L3	L2-L3
☐	4		[12.5.1] Procedimientos de control de cambios				L0-L3	L1-L3	L2-L3
☐	3		[12.5.2] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo				L0-L2	L1-L3	L2-L3
☐	4		[12.5.3] Restricciones a los cambios en los paquetes de software				L0-L2	L2-L3	L2-L3
☐	5		[12.5.4] Fugas de información				L0-L2	L1-L3	L2-L3
☐	4		[12.5.5] Externalización del desarrollo de software				L0-L3	L0-L3	L2-L3
☐	6		[12.6] Gestión de la vulnerabilidad técnica				L0-L3	L0-L3	L2-L4
☐	6		[12.6.1] Control de las vulnerabilidades técnicas				L0-L3	L0-L3	L2-L4
☐	5		[13] Gestión de incidentes de seguridad de la información				L0-L3	L1-L3	L2-L3
☐	3		[13.1] Notificación de eventos y puntos débiles de seguridad de la información				L1-L3	L2-L3	L2-L3
☐	3		[13.1.1] Notificación de eventos de seguridad de la información				L2-L3	L3	L3
☐	3		[13.1.2] Notificación de puntos débiles de seguridad				L1-L2	L2	L2-L3
☐	5		[13.2] Gestión de incidentes de seguridad de la información y mejoras				L0-L3	L1-L3	L2-L3
☐	5		[13.2.1] Responsabilidades y procedimientos				L0-L3	L1-L3	L2-L3
☐	4		[13.2.2] Aprendizaje de los incidentes de seguridad de la información				L0-L2	L1-L3	L2-L3
☐	3		[13.2.3] Recopilación de evidencias				L0-L1	L1-L2	L3

	rec...		control	dud...	apli...	co...	actual	objetivo	PILAR
☐	5		[14] Gestión de la continuidad del negocio				L0-L3	L0-L3	L2-L3
☐	5		[14.1] Aspectos de seguridad de la información en la gestión de la continuidad del negocio				L0-L3	L0-L3	L2-L3
☐	4		[14.1.1] Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio				L0	L1-L2	L2-L3
☐	3		[14.1.2] Continuidad del negocio y evaluación de riesgos				L0-L1	L1-L2	L2-L3
☐	5		[14.1.3] Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información				L0-L3	L0-L3	L2-L3
☐	5		[14.1.4] Marco de referencia para la planificación de la continuidad del negocio				L0-L3	L1-L3	L2-L3
☐	4		[14.1.5] Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio				L0	L0-L1	L3
☐	6		[15] Cumplimiento		...		L0-L3	L1-L3	L2-L4
☐	5		[15.1] Cumplimiento de los requisitos legales		...		L0-L3	L1-L3	L2-L3
☐	2		[15.1.1] Identificación de legislación aplicable				L2	L2	L2
☐	3		[15.1.2] Derechos de propiedad intelectual (IPR)				L1-L2	L2	L2-L3
☐			[15.1.3] Protección de los documentos de la organización		n.a.				
☐	3		[15.1.4] Protección de datos y privacidad de la información de carácter personal				L0-L3	L2-L3	L2-L3
☐	5		[15.1.5] Prevención del uso indebido de los recursos de tratamiento de la información				L0-L3	L1-L3	L2-L3
☐	4		[15.1.6] Regulación de los controles criptográficos				L1	L2	L2-L3
☐	6		[15.2] Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico				L0-L2	L1-L3	L2-L4
☐	2		[15.2.1] Cumplimiento de las políticas y normas de seguridad				L2	L2	L2
☐	2		[G.3.5] Se revisa periódicamente el cumplimiento por parte del personal				L2	L2	L2
☐	6		[15.2.2] Comprobación del cumplimiento técnico				L0-L1	L1-L3	L2-L4
☐	5		[G.exam] Inspecciones de seguridad				L0-L1	L1-L3	L2-L3
☐	6		[H.tools.VA] Herramienta de análisis de vulnerabilidades				L1	L2	L3-L4
☐	5		[15.3] Consideraciones sobre la auditoría de los sistemas de información				L0-L1	L2	L3
☐	5		[15.3.1] Controles de auditoría de los sistemas de información				L0-L1	L2	L3
☐	4		[H.AU.1.2] Gestión de las actividades de registro y auditoría				L0	L2	L3
☐	5		[H.AU.4.2] Consolidación y reporte				L1	L2	L3
☐	3		[15.3.2] Protección de las herramientas de auditoría de los sistemas de información				L0	L2	L3
☐	3		[H.AU.2.1] Protección de las herramientas de auditoría de sistemas				L0	L2	L3

4.2.4. ISO/IEC 27002:2013

Es mostren les pantalles d'avaluació del perfil de la ISO/IEC 27002:2013

[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

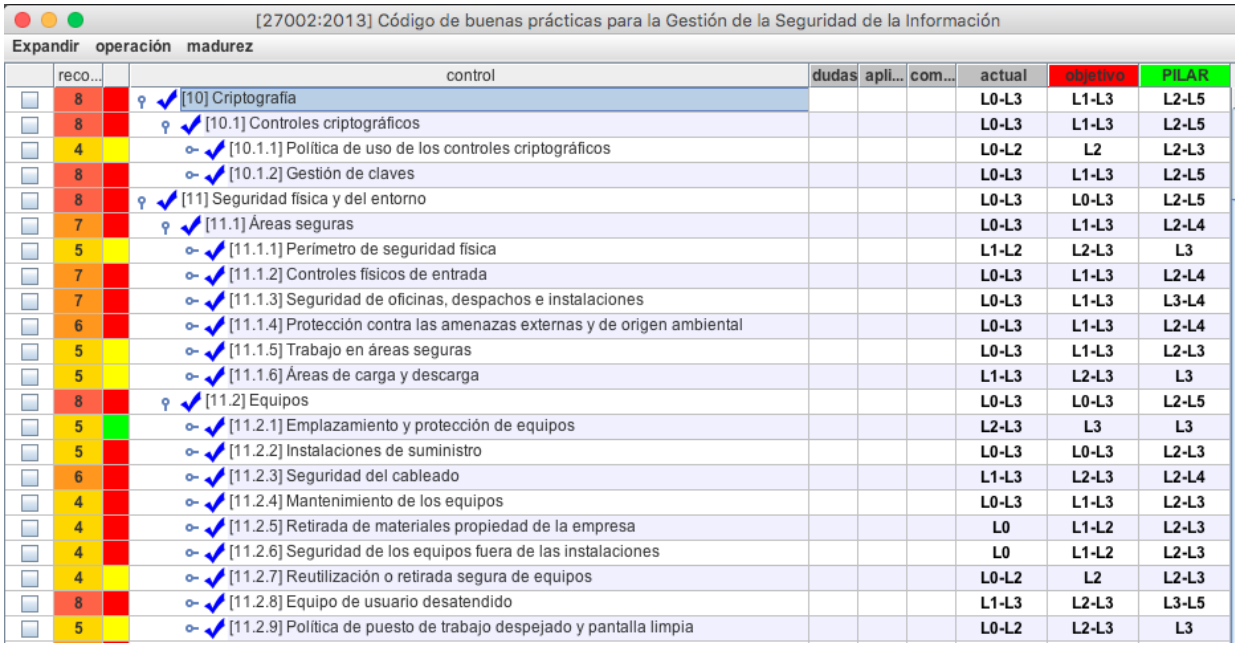
Expandir operación madurez

reco...	control	dudas	apli...	com...	actual	objetivo	PILAR
	[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información				L0-L3	L0-L4	L2-L5
2	[5] Políticas de seguridad de la información				L1-L2	L2	L2
2	[5.1] Dirección de la gestión de la seguridad de la información				L1-L2	L2	L2
2	[5.1.1] Políticas de seguridad de la información				L1-L2	L2	L2
2	[G.3.3] Normas de seguridad				L1-L2	L2	L2
2	[5.1.2] Revisión de las políticas de seguridad de la información				L2	L2	L2
2	[G.3.3.6] Se revisan regularmente				L2	L2	L2
5	[6] Organización de la seguridad de la información				L0-L3	L1-L3	L2-L3
5	[6.1] Organización interna				L0-L3	L2-L3	L2-L3
3	[6.1.1] Roles y responsabilidades relativas a la seguridad de la información				L1-L3	L2-L3	L2-L3
5	[6.1.2] Separación de tareas				L0-L3	L2-L3	L2-L3
3	[6.1.3] Contacto con las autoridades				L2	L3	L3
4	[6.1.4] Contacto con grupos de especial interés				L2-L3	L3	L3
5	[6.1.5] Seguridad de la información en la gestión de proyectos				L2	L3	n.a.
4	[6.2] Dispositivos móviles y teletrabajo				L0-L2	L1-L2	L2-L3
3	[6.2.1] Política de dispositivos móviles				L0-L2	L1-L2	L2-L3
4	[6.2.2] Teletrabajo				L0-L2	L1-L2	L2-L3
6	[7] Seguridad ligada a los recursos humanos				L0-L3	L1-L3	L2-L4
4	[7.1] Antes del empleo				L0-L3	L1-L3	L2-L3
4	[7.1.1] Investigación de antecedentes				L0-L1	L1-L2	L3
3	[7.1.2] Términos y condiciones de contratación				L0-L3	L1-L3	L2-L3
6	[7.2] Durante el empleo				L0-L3	L2-L3	L2-L4
3	[7.2.1] Responsabilidades de la Dirección				L0-L2	L2-L3	L2-L3
6	[7.2.2] Concienciación, formación y capacitación en seguridad de la información				L0-L2	L2	L2-L4
3	[7.2.3] Proceso disciplinario				L1-L3	L2-L3	L2-L3
5	[7.3] Cese del empleo o cambio de puesto de trabajo				L0-L2	L1-L3	L2-L3
5	[7.3.1] Terminación o cambio de responsabilidades laborales				L0-L2	L1-L3	L2-L3

[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Expandir operación madurez

reco...	control	dudas	apli...	com...	actual	objetivo	PILAR
6	[8] Gestión de activos				L0-L3	L1-L3	L2-L4
5	[8.1] Responsabilidad sobre los activos				L0-L3	L1-L3	L2-L3
4	[8.1.1] Inventario de activos				L0-L3	L1-L3	L2-L3
3	[8.1.2] Propiedad de los activos				L0-L2	L1-L3	L2-L3
3	[8.1.3] Uso aceptable de los activos				L0-L3	L1-L3	L2-L3
5	[8.1.4] Devolución de activos				L2	L3	L3
5	[8.2] Clasificación de la información				L0-L2	L1-L3	L2-L3
4	[8.2.1] Clasificación de la información				L0-L2	L1-L2	L2-L3
3	[8.2.2] Marcado de la información				L0	L1-L2	L2-L3
5	[8.2.3] Manejo de activos				L0-L2	L2-L3	L2-L3
6	[8.3] Manipulación de los soportes				L0-L3	L1-L3	L2-L4
5	[8.3.1] Gestión de soportes extraíbles				L0-L3	L2-L3	L2-L3
4	[8.3.2] Retirada de soportes				L0-L2	L2	L2-L3
6	[8.3.3] Transferencia de soportes físicos				L0-L2	L1-L3	L2-L4
8	[9] Control de acceso				L0-L3	L1-L4	L2-L5
5	[9.1] Requisitos de negocio para el control de acceso				L0-L3	L2-L3	L2-L3
5	[9.1.1] Política de control de acceso				L0-L3	L2-L3	L2-L3
2	[9.1.2] Acceso a redes y servicios en red				L1	L2	L2
7	[9.2] Gestión del acceso de usuario				L0-L3	L1-L4	L2-L4
5	[9.2.1] Altas y bajas de usuarios				L2-L3	L3	L3
5	[9.2.2] Gestión de derechos de acceso de los usuarios				L0-L2	L1-L3	L2-L3
6	[9.2.3] Gestión de derechos de acceso especiales				L0-L3	L1-L3	L2-L4
7	[9.2.4] Gestión de la información secreta de autenticación de usuarios				L0-L2	L2-L4	L2-L4
5	[9.2.5] Revisión de derechos de acceso de usuario				L0-L2	L2-L3	L3
5	[9.2.6] Terminación o revisión de los privilegios de acceso				L2	L3	L3
7	[9.3] Responsabilidades de usuario				L2	L4	L4
7	[9.3.1] Uso de la información secreta de autenticación				L2	L4	L4
8	[9.4] Control de acceso al sistema y a las aplicaciones				L0-L3	L1-L3	L2-L5
5	[9.4.1] Restricción del acceso a la información				L2	L2-L3	L2-L3
8	[9.4.2] Procedimientos seguros de inicio de sesión				L0-L3	L2-L3	L3-L5
8	[9.4.3] Gestión de las contraseñas de usuario				L0-L3	L2-L3	L2-L5
5	[9.4.4] Uso de los recursos del sistema con privilegios especiales				L0-L2	L1-L3	L3
4	[9.4.5] Control de acceso al código fuente de los programas				L0-L2	L1-L3	L2-L3



[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Expandir operación madurez

reco...	control	dudas	apli...	com...	actual	objetivo	PILAR
8	[10] Criptografía				L0-L3	L1-L3	L2-L5
8	[10.1] Controles criptográficos				L0-L3	L1-L3	L2-L5
4	[10.1.1] Política de uso de los controles criptográficos				L0-L2	L2	L2-L3
8	[10.1.2] Gestión de claves				L0-L3	L1-L3	L2-L5
8	[11] Seguridad física y del entorno				L0-L3	L0-L3	L2-L5
7	[11.1] Áreas seguras				L0-L3	L1-L3	L2-L4
5	[11.1.1] Perímetro de seguridad física				L1-L2	L2-L3	L3
7	[11.1.2] Controles físicos de entrada				L0-L3	L1-L3	L2-L4
7	[11.1.3] Seguridad de oficinas, despachos e instalaciones				L0-L3	L1-L3	L3-L4
6	[11.1.4] Protección contra las amenazas externas y de origen ambiental				L0-L3	L1-L3	L2-L4
5	[11.1.5] Trabajo en áreas seguras				L0-L3	L1-L3	L2-L3
5	[11.1.6] Áreas de carga y descarga				L1-L3	L2-L3	L3
8	[11.2] Equipos				L0-L3	L0-L3	L2-L5
5	[11.2.1] Emplazamiento y protección de equipos				L2-L3	L3	L3
5	[11.2.2] Instalaciones de suministro				L0-L3	L0-L3	L2-L3
6	[11.2.3] Seguridad del cableado				L1-L3	L2-L3	L2-L4
4	[11.2.4] Mantenimiento de los equipos				L0-L3	L1-L3	L2-L3
4	[11.2.5] Retirada de materiales propiedad de la empresa				L0	L1-L2	L2-L3
4	[11.2.6] Seguridad de los equipos fuera de las instalaciones				L0	L1-L2	L2-L3
4	[11.2.7] Reutilización o retirada segura de equipos				L0-L2	L2	L2-L3
8	[11.2.8] Equipo de usuario desatendido				L1-L3	L2-L3	L3-L5
5	[11.2.9] Política de puesto de trabajo despejado y pantalla limpia				L0-L2	L2-L3	L3

[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Expandir operación madurez

reco...	control	dudas	apli...	com...	actual	objetivo	PILAR
7	[12] Gestión de operaciones				L0-L3	L0-L3	L2-L4
5	[12.1] Responsabilidades y procedimientos de operación				L0-L3	L1-L3	L2-L3
3	[12.1.1] Documentación de los procedimientos de operación				L0-L2	L2-L3	L2-L3
5	[12.1.2] Gestión de cambios				L0-L3	L1-L3	L2-L3
3	[12.1.3] Gestión de capacidades				L0-L2	L1-L2	L2-L3
4	[12.1.4] Separación de los entornos de desarrollo, prueba y operación				L0-L3	L1-L3	L2-L3
7	[12.2] Protección contra el código malicioso				L0-L3	L2-L3	L2-L4
7	[12.2.1] Controles contra el código malicioso				L0-L3	L2-L3	L2-L4
5	[12.3] Copias de seguridad				L0-L3	L2-L3	L2-L3
5	[12.3.1] Copias de seguridad de la información				L0-L3	L2-L3	L2-L3
6	[12.4] Registro y monitorización				L0-L3	L1-L3	L2-L4
5	[12.4.1] Registro de eventos				L0-L3	L1-L3	L2-L3
5	[12.4.2] Protección de la información de los registros				L0-L3	L2-L3	L3
2	[12.4.3] Registros de administración y operación				L1	L2	L2
6	[12.4.4] Sincronización del reloj				L1-L3	L2-L3	L3-L4
7	[12.5] Control del software en explotación				L0-L3	L1-L3	L2-L4
7	[12.5.1] Instalación de software en sistemas operacionales				L0-L3	L1-L3	L2-L4
6	[12.6] Gestión de las vulnerabilidades técnicas				L0-L3	L0-L3	L2-L4
6	[12.6.1] Control de las vulnerabilidades técnicas				L0-L3	L0-L3	L2-L4
3	[12.6.2] Restricciones a la instalación de software				L0-L2	L2-L3	L2-L3
5	[12.7] Consideraciones sobre la auditoría de los sistemas de información				L0-L1	L2	L3
5	[12.7.1] Controles de auditoría de los sistemas de información				L0-L1	L2	L3
8	[13] Seguridad de las comunicaciones	...			L0-L3	L1-L3	L2-L5
8	[13.1] Gestión de la seguridad de las redes	...			L0-L3	L2-L3	L2-L5
5	[13.1.1] Controles de red				L0-L3	L2-L3	L2-L3
8	[13.1.2] Seguridad de los servicios de red	...			L0-L3	L2-L3	L2-L5
6	[13.1.3] Segregación de redes				L3	L3	L3-L4
5	[13.2] Transferencia de información				L0-L3	L1-L3	L2-L3
3	[13.2.1] Políticas y procedimientos de transferencia de información				L0-L1	L1-L2	L3
5	[13.2.2] Acuerdos de transferencia de información				L1-L2	L1-L3	L2-L3
4	[13.2.3] Mensajería electrónica				L0-L3	L2-L3	L2-L3
3	[13.2.4] Acuerdos de confidencialidad o no divulgación				L1	L2-L3	L2-L3

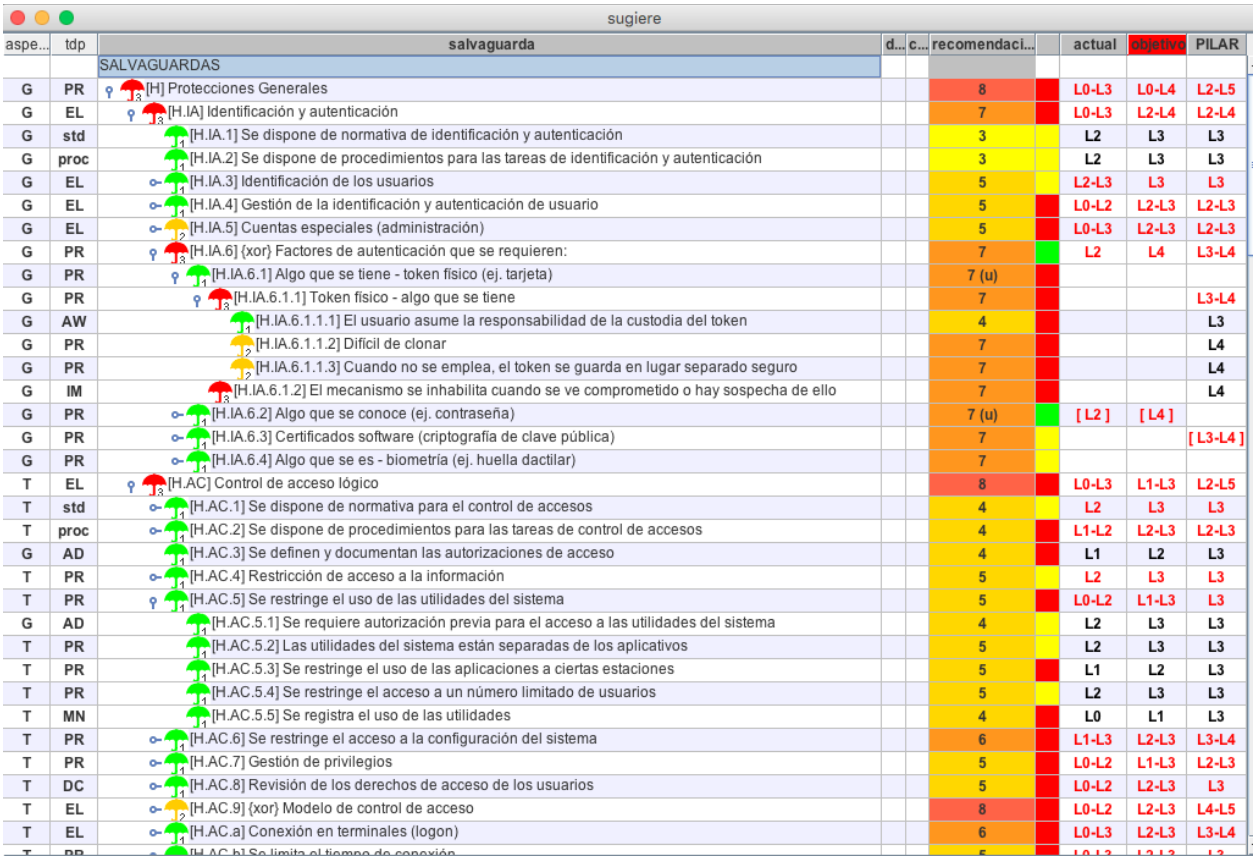
[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Expandir operación madurez

	reco...		control	dudas	aplic...	com...	actual	objetivo	PILAR
	6		[14] Adquisición, desarrollo y mantenimiento de los sistemas				L0-L3	L0-L3	L2-L4
	6		[14.1] Requisitos de seguridad de los sistemas de información				L0-L3	L1-L3	L2-L4
	3		[14.1.1] Análisis y especificación de los requisitos de seguridad				L0-L2	L2	L2-L3
	5		[14.1.2] Aseguramiento de servicios y aplicaciones en redes públicas				L0-L3	L2-L3	L2-L3
	6		[14.1.3] Protección de las transacciones				L0-L3	L1-L3	L2-L4
	4		[14.2] Seguridad en los procesos de desarrollo y soporte				L0-L3	L0-L3	L2-L3
	4		[14.2.1] Política de desarrollo seguro				L0-L3	L0-L3	L2-L3
	4		[14.2.2] Procedimientos de control de cambios en el sistema				L0-L3	L1-L3	L2-L3
	3		[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma				L0-L2	L1-L3	L2-L3
	4		[14.2.4] Restricciones a los cambios en los paquetes de software				L0-L2	L2-L3	L2-L3
	3		[14.2.5] Principios para la ingeniería de sistemas seguros				L0-L2	L1-L3	L3
	4		[14.2.6] Entorno de desarrollo seguro				L0-L3	L1-L3	L3
	4		[14.2.7] Externalización del desarrollo de software				L0-L2	L1-L3	L2-L3
	4		[14.2.8] Pruebas de seguridad del sistema				L0-L3	L2-L3	L2-L3
	4		[14.2.9] Pruebas de aceptación del sistema				L0-L3	L0-L3	L3
	4		[14.3] Datos de prueba				L3	L3	L3
	4		[14.3.1] Protección de los datos de prueba				L3	L3	L3
	5		[15] Relaciones con proveedores				L0-L3	L1-L3	L2-L3
	3		[15.1] Seguridad de la información en las relaciones con proveedores				L0-L3	L1-L3	L2-L3
	2		[15.1.1] Política de seguridad de la información en las relaciones con proveedores				L1-L3	L2-L3	L2
	3		[15.1.2] Tratamiento de la seguridad en contratos con proveedores				L0-L3	L1-L3	L2-L3
	2		[15.1.3] Cadena de suministro de tecnologías de la información y comunicaciones				L0-L2	L1-L2	L2
	5		[15.2] Gestión de servicios prestados por terceros				L0-L3	L1-L3	L2-L3
	5		[15.2.1] Supervisión y revisión de los servicios prestados por terceros				L0-L3	L1-L3	L2-L3
	2		[15.2.2] Gestión del cambio en los servicios prestados por terceros				L1-L2	L2	L2
	5		[16] Gestión de incidentes de seguridad de la información				L0-L3	L1-L3	L2-L3
	5		[16.1] Gestión de incidentes de seguridad de la información y mejoras				L0-L3	L1-L3	L2-L3
	5		[16.1.1] Responsabilidades y procedimientos				L0-L2	L1-L3	L2-L3
	3		[16.1.2] Notificación de eventos de seguridad de la información				L2-L3	L3	L3
	3		[16.1.3] Notificación de puntos débiles de seguridad				L1-L2	L2	L2-L3
	3		[16.1.4] Evaluación y decisión respecto de los eventos de seguridad de la información				L1-L2	L2	L2-L3
	5		[16.1.5] Respuesta a incidentes de seguridad de la información				L0-L3	L1-L3	L2-L3
	4		[16.1.6] Aprendizaje de los incidentes de seguridad de la información				L0-L2	L1-L3	L2-L3
	3		[16.1.7] Recopilación de evidencias				L0-L1	L1-L2	L3
	5		[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio				L0-L3	L0-L3	L2-L3
	5		[17.1] Continuidad de la seguridad de la información				L0-L3	L0-L3	L2-L3
	4		[17.1.1] Planificar la continuidad de la seguridad de la información				L0	L1-L2	L2-L3
	5		[17.1.2] Implementar la continuidad de la seguridad de la información				L0-L3	L0-L3	L2-L3
	4		[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información				L0	L0-L1	L3
	5		[17.2] Redundancia				L0-L3	L0-L3	L2-L3
	5		[17.2.1] Disponibilidad de los medios de procesamiento de información				L0-L3	L0-L3	L2-L3
	6		[18] Cumplimiento		...		L0-L3	L1-L3	L2-L4
	4		[18.1] Cumplimiento de los requisitos legales y contractuales		...		L0-L3	L2-L3	L2-L3
	2		[18.1.1] Identificación de legislación aplicable y requisitos contractuales				L2	L2	L2
	3		[18.1.2] Derechos de propiedad intelectual (IPR)				L1-L2	L2	L2-L3
			[18.1.3] Protección de los documentos de la organización		n.a.				
	3		[18.1.4] Protección de datos y privacidad de la información de carácter personal				L0-L3	L2-L3	L2-L3
	4		[18.1.5] Regulación de los controles criptográficos				L1	L2	L2-L3
	6		[18.2] Revisiones de seguridad de la información				L0-L2	L1-L3	L2-L4
	5		[18.2.1] Revisión independiente de la seguridad de la información				L0-L1	L1-L2	L2-L3
	2		[18.2.2] Cumplimiento de las políticas y normas de seguridad				L2	L2	L2
	6		[18.2.3] Comprobación del cumplimiento técnico				L0-L1	L1-L3	L2-L4

4.2.5. Salvaguardes

Un dels resultats de l'avaluació utilitzant l'eina és una llista de les salvaguardes a aplicar i el seu grau de madures per a cada fase (actual, objectiu i PILAR).



aspe...	tdp	salvaguarda	d...	c...	recomendaci...	actual	objetivo	PILAR
		SALVAGUARDAS						
G	PR	[H] Protecciones Generales			8	L0-L3	L0-L4	L2-L5
G	EL	[H.IA] Identificación y autenticación			7	L0-L3	L2-L4	L2-L4
G	std	[H.IA.1] Se dispone de normativa de identificación y autenticación			3	L2	L3	L3
G	proc	[H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación			3	L2	L3	L3
G	EL	[H.IA.3] Identificación de los usuarios			5	L2-L3	L3	L3
G	EL	[H.IA.4] Gestión de la identificación y autenticación de usuario			5	L0-L2	L2-L3	L2-L3
G	EL	[H.IA.5] Cuentas especiales (administración)			5	L0-L3	L2-L3	L2-L3
G	PR	[H.IA.6] {xor} Factores de autenticación que se requieren:			7	L2	L4	L3-L4
G	PR	[H.IA.6.1] Algo que se tiene - token físico (ej. tarjeta)			7 (u)			
G	PR	[H.IA.6.1.1] Token físico - algo que se tiene			7			L3-L4
G	AW	[H.IA.6.1.1.1] El usuario asume la responsabilidad de la custodia del token			4			L3
G	PR	[H.IA.6.1.1.2] Difícil de clonar			7			L4
G	PR	[H.IA.6.1.1.3] Cuando no se emplea, el token se guarda en lugar separado seguro			7			L4
G	IM	[H.IA.6.1.2] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello			7			L4
G	PR	[H.IA.6.2] Algo que se conoce (ej. contraseña)			7 (u)	[L2]	[L4]	
G	PR	[H.IA.6.3] Certificados software (criptografía de clave pública)			7			[L3-L4]
G	PR	[H.IA.6.4] Algo que se es - biometría (ej. huella dactilar)			7			
T	EL	[H.AC] Control de acceso lógico			8	L0-L3	L1-L3	L2-L5
T	std	[H.AC.1] Se dispone de normativa para el control de accesos			4	L2	L3	L3
T	proc	[H.AC.2] Se dispone de procedimientos para las tareas de control de accesos			4	L1-L2	L2-L3	L2-L3
G	AD	[H.AC.3] Se definen y documentan las autorizaciones de acceso			4	L1	L2	L3
T	PR	[H.AC.4] Restricción de acceso a la información			5	L2	L3	L3
T	PR	[H.AC.5] Se restringe el uso de las utilidades del sistema			5	L0-L2	L1-L3	L3
G	AD	[H.AC.5.1] Se requiere autorización previa para el acceso a las utilidades del sistema			4	L2	L3	L3
T	PR	[H.AC.5.2] Las utilidades del sistema están separadas de los aplicativos			5	L2	L3	L3
T	PR	[H.AC.5.3] Se restringe el uso de las aplicaciones a ciertas estaciones			5	L1	L2	L3
T	PR	[H.AC.5.4] Se restringe el acceso a un número limitado de usuarios			5	L2	L3	L3
T	MN	[H.AC.5.5] Se registra el uso de las utilidades			4	L0	L1	L3
T	PR	[H.AC.6] Se restringe el acceso a la configuración del sistema			6	L1-L3	L2-L3	L3-L4
T	PR	[H.AC.7] Gestión de privilegios			5	L0-L2	L1-L3	L2-L3
T	DC	[H.AC.8] Revisión de los derechos de acceso de los usuarios			5	L0-L2	L2-L3	L3
T	EL	[H.AC.9] {xor} Modelo de control de acceso			8	L0-L2	L2-L3	L4-L5
T	EL	[H.AC.a] Conexión en terminales (logon)			6	L0-L3	L2-L3	L3-L4

La relació complerta de totes les salvaguardes contemplades extretes de l'eina PILAR es detalla a l'annex VI de salvaguardes.

4.3. Avaluació impacte potencial

4.3.1. Impacte potencial

Es denomina impacte a la mesura del dany sobre l'actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius en vàries dimensions i la degradació que causarien les amenaces es pot derivar l'impacte que aquestes tindrien sobre el sistema.

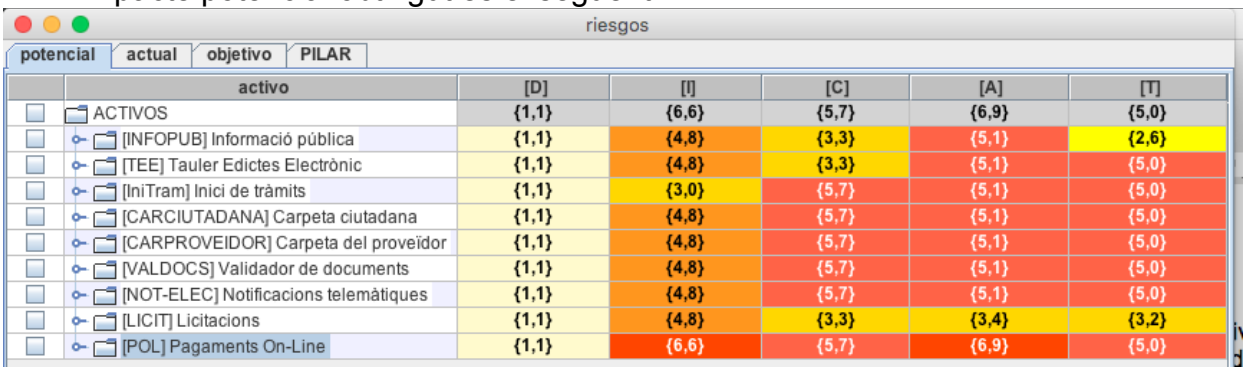
L'impacte potencial no contempla l'aplicació de cap salvaguarda. L'eina µPILAR realitza el càlcul de:

- impacte potencial (inicial del sistema sense contemplar cap salvaguarda)
- impacte actual (el rel un cop aplicades les salvaguardes al nivell actual)
- impacte objectiu (les que es volen obtenir com a objectiu)
- impacte PILAR (el que l'eina recomana que hauríem de tenir finalment)

El risc es mesura en una escala entre 0,0 i 10,0 seguint els criteris següents:

9 - NIVEL 9
8 - NIVEL 8
7 - extremadamente crítico
6 - muy crítico
5 - crítico
4 - muy alto
3 - alto
2 - medio
1 - bajo
0 - despreciable

L'impacte potencial obtingut és el següent:



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{1,1}	{6,6}	{5,7}	{6,9}	{5,0}
[INFOPUB] Informació pública	{1,1}	{4,8}	{3,3}	{5,1}	{2,6}
[TEE] Tauler Edictes Electrònic	{1,1}	{4,8}	{3,3}	{5,1}	{5,0}
[IniTram] Inici de tràmits	{1,1}	{3,0}	{5,7}	{5,1}	{5,0}
[CARCIUTADANA] Carpeta ciutadana	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[CARPROVEIDOR] Carpeta del proveïdor	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[VALDOCS] Validador de documents	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[NOT-ELEC] Notificacions telemàtiques	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[LICIT] Licitacions	{1,1}	{4,8}	{3,3}	{3,4}	{3,2}
[POL] Pagaments On-Line	{1,1}	{6,6}	{5,7}	{6,9}	{5,0}

Tenim **2** valoracions "**Molt crítiques**" (la Integritat i l'Autenticitat al servei de pagament on-line), **20** valoracions "**Crítiques**", **7** de "**Molt altes**", **6** "**Altes**" i 9 entre "mitjanes" i "Baixes". El risc intrínsec recollit a l'impacte potencial és molt alt ja que si la direcció assumeix que el risc acceptable és qualsevol igual o inferior a "mitjà" llavors hi ha 35 valoracions per sobre del nivell acceptable i s'han de reduir.

Aquest és el risc potencial o teòric del nostre sistema. Tenim desplegades unes salvaguardes o controls i hem de veure com redueixen aquest risc i el resultat serà el "risc real" o "risc efectiu" i correspondrà a l'impacte actual del nostre sistema.

4.3.2. Impacte actual

És l'impacte potencial valorat després d'aplicar-li les salvaguardes i que correspon al "risc real" o "risc efectiu" del nostre sistema en el moment actual.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}
[INFOPUB] Informació pública	{0,62}	{3,4}	{1,3}	{3,6}	{1,1}
[TEE] Tauler Edictes Electrònic	{0,62}	{3,4}	{1,3}	{3,6}	{3,4}
[IniTram] Inici de tràmits	{0,62}	{1,6}	{3,7}	{3,6}	{3,4}
[CARCIUTADANA] Carpeta ciutadana	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[CARPROVEIDOR] Carpeta del proveïdor	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[VALDOCS] Validador de documents	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[NOT-ELEC] Notificacions telemàtiques	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[LICIT] Licitacions	{0,62}	{3,4}	{1,3}	{1,8}	{1,7}
[POL] Pagaments On-Line	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}

Aquí podem veure que la situació ha variat molt respecte a l'impacte potencial.

- Hem passat de tenir 2 valoracions "Molt crítiques" a no tenir-ne cap.
- Hem passat de tenir 20 valoracions "Crítiques" a tenir-ne 2.
- Hem passat de tenir 7 valoracions "Molt altes" a no tenir-ne cap.
- Hem passat de tenir 6 valoracions "Altes" a tenir-ne 27.

De les 22 valoracions "Molt crítiques" o "Crítiques" realment només en tenim 2. La resta de riscos teòrics s'han vist reduïts per l'efectivitat de les salvaguardes que ja s'estaven prenent en el sistema. Aquestes criticitats s'han vist reduïdes a la pràctica a riscos de nivell "Alt". La qual deixa una foto inicial del nostre sistema molt millor que la que dibuixava l'impacte potencial.

El nivell i valors d'aquestes valoracions ens indicaran quins són els primers controls i salvaguardes s'han d'implantar per a reduir el risc als nivells que decideixi la direcció de la nostra organització. En el cas concret que ens ocupa aquesta decisió l'ha de prendre el "Comitè de Seguretat".

Abans de centrar-nos en quin ha de ser el nostre nivell de risc acceptable i quin serà el nivell de risc residual que romandrà al nostre sistema, analitzarem els impactes que ens ofereix l'eina PILAR corresponents a "impacte objectiu" i a "Impacte PILAR".

4.3.3. Impacte objectiu

Aquest és l'impacte potencial valorat després d'aplicar-li les salvaguardes i contramesures descrites a la valoració "Objectiu" i que estarien emmarcades a un període limitat en el temps per a la seva aplicació. Aquest període podria ser d'un any o mig any i aniria en concordància a la planificació realitzada a la fase de "Propostes de projectes".

Tot i anomenar-se "Objectiu" l'escenari dibuixat per aquest avaluació d'impacte no correspondria a la fase final a la que volem arribar sinó a una fase intermèdia per la qual hem de passar per a arribar al nostre objectiu final que correspondria a la fase anomenada "PILAR".

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,40}	{3,7}	{2,6}	{3,8}	{2,1}
[INFOPUB] Informació pública	{0,40}	{1,9}	{0,84}	{2,0}	{0,74}
[TEE] Tauler Edictes Electrònic	{0,40}	{1,9}	{0,84}	{2,0}	{2,1}
[IniTram] Inici de tràmits	{0,40}	{0,82}	{2,6}	{2,0}	{2,1}
[CARCIUTADANA] Carpeta ciutadana	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[CARPROVEIDOR] Carpeta del proveïdor	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[VALDOCS] Validador de documents	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[NOT-ELEC] Notificacions telemàtiques	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[LICIT] Licitacions	{0,40}	{1,9}	{0,84}	{0,85}	{0,85}
[POL] Pagaments On-Line	{0,40}	{3,7}	{2,6}	{3,8}	{2,1}

Es constata que al final de la fase objectiu no hi ha valoracions de nivell "Crític" o "Molt alt".

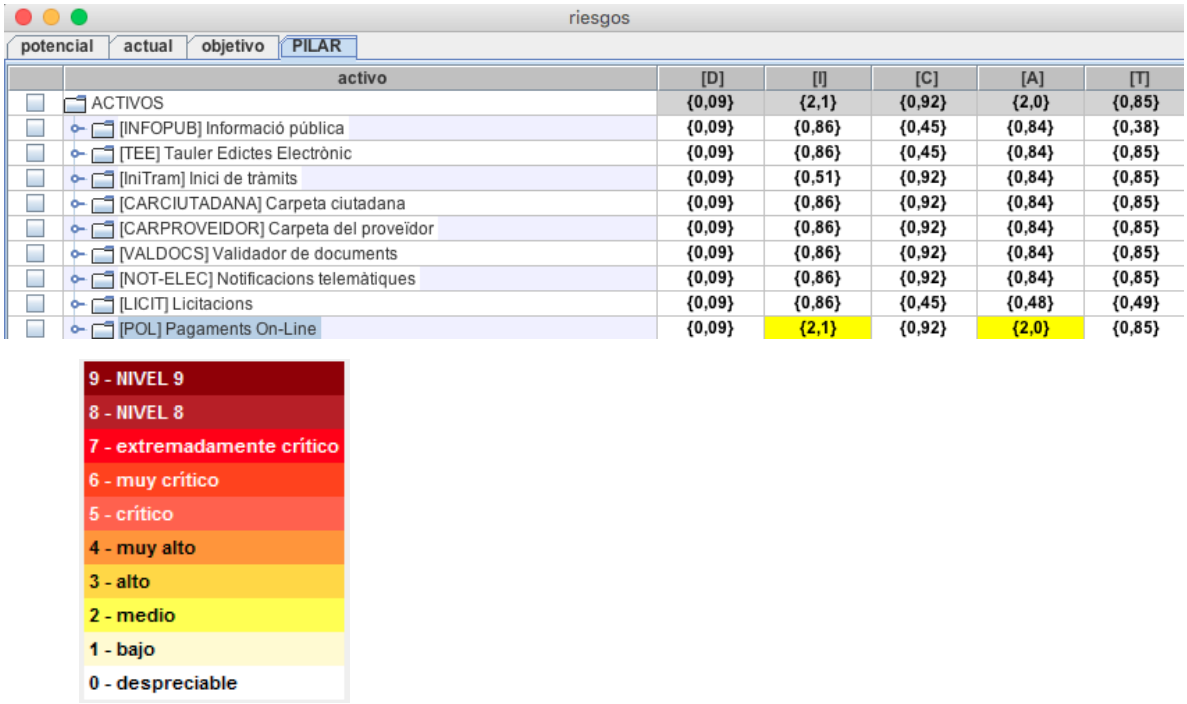
El resultat, comparativament respecte al "risc actual" és:

- Hem passat de tenir 2 valoracions "Crítiques" a no tenir-ne cap.
- Hem passat de tenir 7 valoracions "Molt altes" a no tenir-ne cap.
- Hem passat de tenir 27 valoracions "Altes" a tenir-ne 2.
- Queden 19 valoracions "mitjanes" i 7 de "baixes" en el sistema.

4.3.4. Impacte recomanat per µPILAR

L'impacte recomanat per PILAR correspon al fet que l'eina que utilitzem segueix la metodologia MAGERIT i aquesta fa unes recomanacions sobre quin hauria de ser el nivell de risc acceptable i quin és el seu impacte sobre les diferents dimensions de seguretat (Disponibilitat, Integritat, Confidencialitat, Autenticitat i Traçabilitat).

Aquest impacte correspondria a l'objectiu real final del nostre sistema (no confondre'l amb la fase que l'eina anomena "Objectiu") i que resultarà després d'aplicar un segon paquet de refinament i aplicació de salvaguardes i contramesures que es descriuen a la fase "PILAR". El període d'execució i desplegament d'aquestes salvaguardes i contramesures hauria de ser el mateix període que es va establir per a la implantació entre les fases "Actual" i "Objectiu".



El resultat, comparativament respecte al "risc objectiu" és:

- Hem passat de tenir 27 valoracions "Altes" a no tenir-ne cap.
- Hem passat de tenir 19 valoracions "Mitjanes" a tenir-ne 2.
- Hem passat de tenir 7 valoracions "Baixes" a no tenir-ne cap.

L'escenari dibuixat és el d'un sistema "sota control" amb només dues valoracions de nivell "Mig" que afecten al servei de "Pagament On-Line" en les dimensions d'Integritat i Autenticitat.

La implantació d'un SGSI implica l'adopció d'un cicle de millora contínua PDCA que revisarà l'efectivitat i aplicació dels controls i les seves salvaguardes per a implantar mesures que redueixin totes les valoracions a nivells 0 o menyspreable.

4.3.5. Risc acceptable i risc residual

Un cop s'han determinat els diferents impactes sobre el nostre sistema cal que l'organització decideixi quin és el nivell de risc que vol acceptar. Aquesta decisió marcarà una frontera entre el que l'organització accepta com a risc raonable i anomenem "risc residual", i contra el qual no implantarà cap mesura correctora, i el que són riscos que l'organització no accepta i contra els quals prendrà mesures correctores amb l'objectiu de reduir-los fins als nivells que consideri acceptables.

Aquesta decisió en una administració pública a l'estat espanyol la legislació, en concret el RD 3/2011 que regula l'Esquema Nacional de Seguretat (en endavant ENS), li atorga al "Comitè de Seguretat". L'ENS no deixa llibertat al "Comitè de Seguretat" per a que decideixi quin és el nivell de risc acceptable sinó que li marca uns mínims que ha de complir i un termini per a adaptar-s'hi. Aquests mínims són els que estan representats a l'eina utilitzada com a fase "PILAR". El termini per a adaptar-s'hi era el 1 de gener de 2015, encara que moltes organitzacions, com el nostre Ajuntament, encara no han finalitzat aquest procés.

En l'anàlisi realitzat, l'eina μPILAR estava configurada per a avaluar la norma ISO/IEC 27002 i no pas l'ENS. Per tant, les recomanacions que proposa PILAR són les que recomana per a la implantació de l'ISO/IEC 27002:2013.

Tenint en compte que les recomanacions de l'eina PILAR es basen en l'experiència acumulada de moltes organitzacions i són recomanacions sobradament contrastades es proposa que el "Comitè de Seguretat" en la implantació del seu SGSI a la ISO/IEC 27002:2013 prengui com a "Risc acceptable" les recomanacions de seguretat de l'eina Pilar que conduiran a una avaluació dels riscos a un nivell 0 o menyspreable.

No es pot oblidar que no hem posat en l'estudi tots els dominis que vam comentar a la fase inicial ni hem considerat tots els actius que té la nostra organització. Només s'ha considerat el subdomini "Seu electrònica". La implantació del SGSI implicarà l'adopció d'un cicle de millora contínua PDCA que revisarà l'efectivitat del sistema de forma anual. Es recomana que cada any en el procés d'inici d'una nova fase de revisió del cicle s'incorpori un nou domini i es faci l'anàlisi de riscos. D'aquesta manera i de forma progressiva aconseguirem que tots els sistemes inclosos en la nostra organització siguin gestionats pel nostre SGSI.

És molt probable que quan incorporem nous subdominis amb els seus actius la valoració inicial que es faci no sigui tan bona com la que s'ha obtingut per al subdomini "Seu electrònica" i surtin uns nivells de no compliment amb les recomanacions molt més elevat.

4.3.6. Resum executiu de l'Anàlisi de Riscos

L'impacte potencial que és aquell que es calcula sense tenir en compte cap de les salvaguardes de les que disposa el nostre sistema. És una dada teòrica que serveix per a que puguem avaluar la bondat de les mesures de seguretat que estem aplicant actualment. El risc residual que accepta la nostra organització és el proposat per l'eina PILAR i està definit en la fase anomenada "PILAR".

L'impacte "actual" és el que mostra l'estat real del risc del nostre sistema. En la nostra anàlisi s'han definit, utilitzant l'eina PILAR, una fase "objectiu" que serà l'estat al que voldrem arribar en un període determinat de temps que hem considerat de 12 mesos. Al final d'aquesta fase encara no haurem assolit els nivells de seguretat que determina la norma ISO/IEC 27002:2013 però ens hi trobarem més a prop.

Els nivells de seguretat que l'eina PILAR recomana per a la implantació de la norma es poden veure en la fase anomenada "PILAR". La transició entre la fase "Objectiu" i la fase "PILAR" hauria de durar aproximadament el mateix que per a la fase anterior, un any.

S'haurà de definir un "Pla de Millora de la Seguretat" amb un conjunt d'actuacions de millora concretes i planificades en el temps que portin el nostre sistema per sota dels límits que marcarà el risc residual acceptats per la nostra organització.

Anem a analitzar els principals riscos a que està sotmesa la nostra organització en el domini "Seu Electrònica". Aquests riscos estan definits a la "fase actual" que correspon a l'impacte potencial valorat després d'aplicar les salvaguardes i que correspon al "risc real" o "risc efectiu" del nostre sistema en el moment actual.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}
[INFOPUB] Informació pública	{0,62}	{3,4}	{1,3}	{3,6}	{1,1}
[TEE] Tauler Edictes Electrònic	{0,62}	{3,4}	{1,3}	{3,6}	{3,4}
[IniTram] Inici de tràmits	{0,62}	{1,6}	{3,7}	{3,6}	{3,4}
[CARCIUTADANA] Carpeta ciutadana	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[CARPROVEIDOR] Carpeta del proveïdor	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[VALDOCS] Validador de documents	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[NOT-ELEC] Notificacions telemàtiques	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[LICIT] Licitacions	{0,62}	{3,4}	{1,3}	{1,8}	{1,7}
[POL] Pagaments On-Line	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}

L'impacte de la "fase actual" ens marca en la seva valoració numèrica quins han de ser els primers objectius a abordar per a reduir els riscos. Els valors més alts són els que indiquen un ris major i per tant els primers sobre els quals hauríem d'aplicar accions de millora.

Tenim **2** valoracions "**Crítiques**" (la Integritat i l'Autenticitat al servei de pagament on-line). Hi ha **27** valoracions "**Altes**" que afecten tots els serveis de forma força homogènia en la Integritat, la Confidencialitat, l'Autenticitat i la Traçabilitat. També n'hi ha **6** de "**Baixes**".

Les primeres accions de millora aniran dirigides a minimitzar els riscs associats amb **l'autenticació** i la **integritat** dels **Pagaments On-Line**. En el cas de l'autenticació cal parar atenció a la gestió de les credencials d'autenticació i les dades de configuració i gestió interna del servei. En el cas de la integritat les mesures faran referència a la gestió de la informació (fitxers de dades, còpies de seguretat, dades de configuració i gestió, aplicacions de gestió, ..) així com dels seus suports (emmagatzemament en xarxa, discos físics i virtuals).

La resta de riscos tenen una distribució homogènia. Això indica que caldrà aplicar una millora global dels controls del sistema per a reduir-los.

Només la Disponibilitat està per sota del nivell de risc residual desitjat. Val a dir que això no és degut al fet que el nostre sistema tingui unes salvaguardes molt ben definides i aplicades sinó al fet que la "Seu electrònica" no és crítica en la seva dimensió de "Disponibilitat". Tots els serveis que s'ofereixen poden patir interrupcions sense que generi un perjudici greu a l'usuari que no es pugui corregir o subsanar.

4.3.7. Anàlisi de Riscos de l'eina PIlar

L'eina µPILAR proporciona 3 llistats o informes predefinits:

- Anàlisi de riscos
- Declaració d'aplicabilitat
- Compliment de la norma

Aquests 3 informes són una de les avantatges de la utilització de l'eina ja que la seva realització es fa utilitzant metodologies contrastades i són comparables a la d'altres organitzacions que utilitzin la mateixa eina.

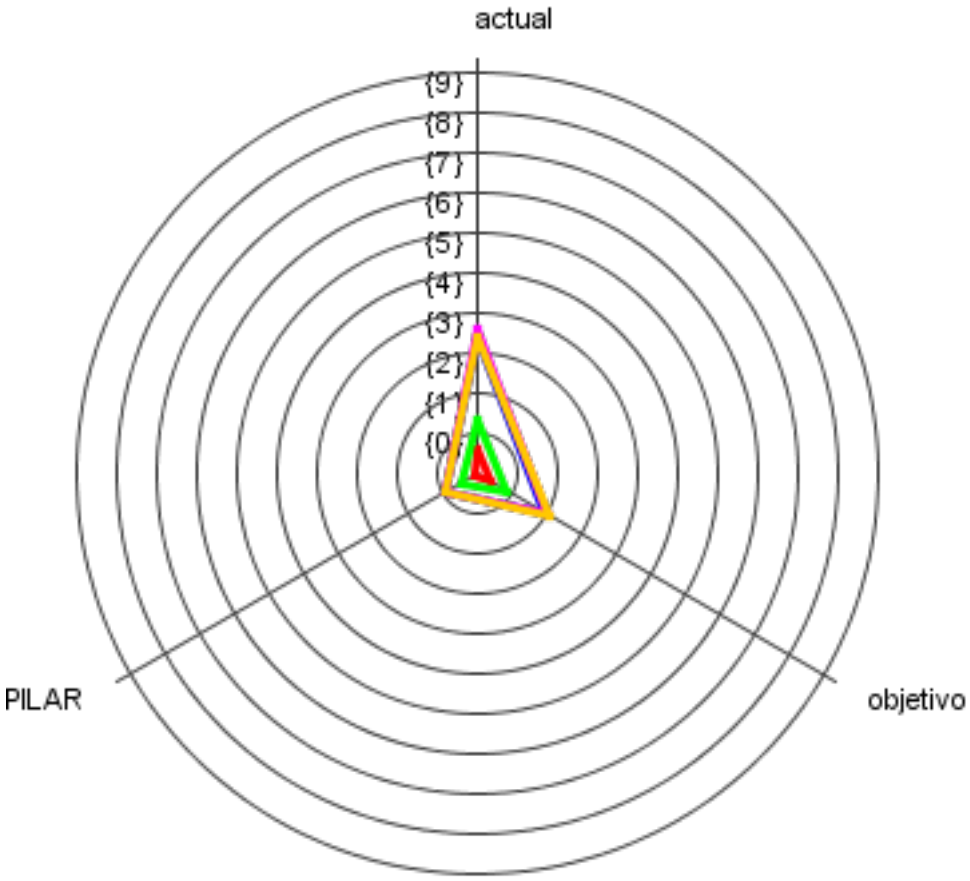
L'informe d'anàlisi de riscos mostra una valoració gràfica del sistema que mostra l'impacte potencial i després mosta per a cada actiu essencial la valoració sobre les 5 dimensions de seguretat per les fases "actual", "objectiu" i "Pilar". Es pot consultat la totalitat de l'informe a l'Annex VII – Anàlisi de riscos PILAR. Es mostra un exemple de la valoració de l'informe per a l'actiu Tauler Edictes Electrònic com un avançament del document de l'annex.

L'informe de Declaració d'aplicabilitat conté la relació de controls de la norma ISO/IEC 27002:2013 i especifica si són o no són d'aplicació. El contingut és pot consultar íntegrament a l'Annex V – Informe declaració d'aplicabilitat PILAR.

L'informe de compliment de la Norma conté l'anàlisi diferencial equivalent a l'Anàlisi de Compliment Inicial calculat manualment en la contextualització de l'empresa. La presentació es fa en el format del Model de Maduresa de la Capacitat CMM i que manté unes equivalències amb un percentatges de compliment de la norma. Es pot consultar l'informe complert a l'Annex IV – Compliment de la Norma 27002:2013 PILAR.

4.3.7.1. Exemple d'anàlisi de risc d'un actiu

[TEE] Tauler Edictes Electrònic



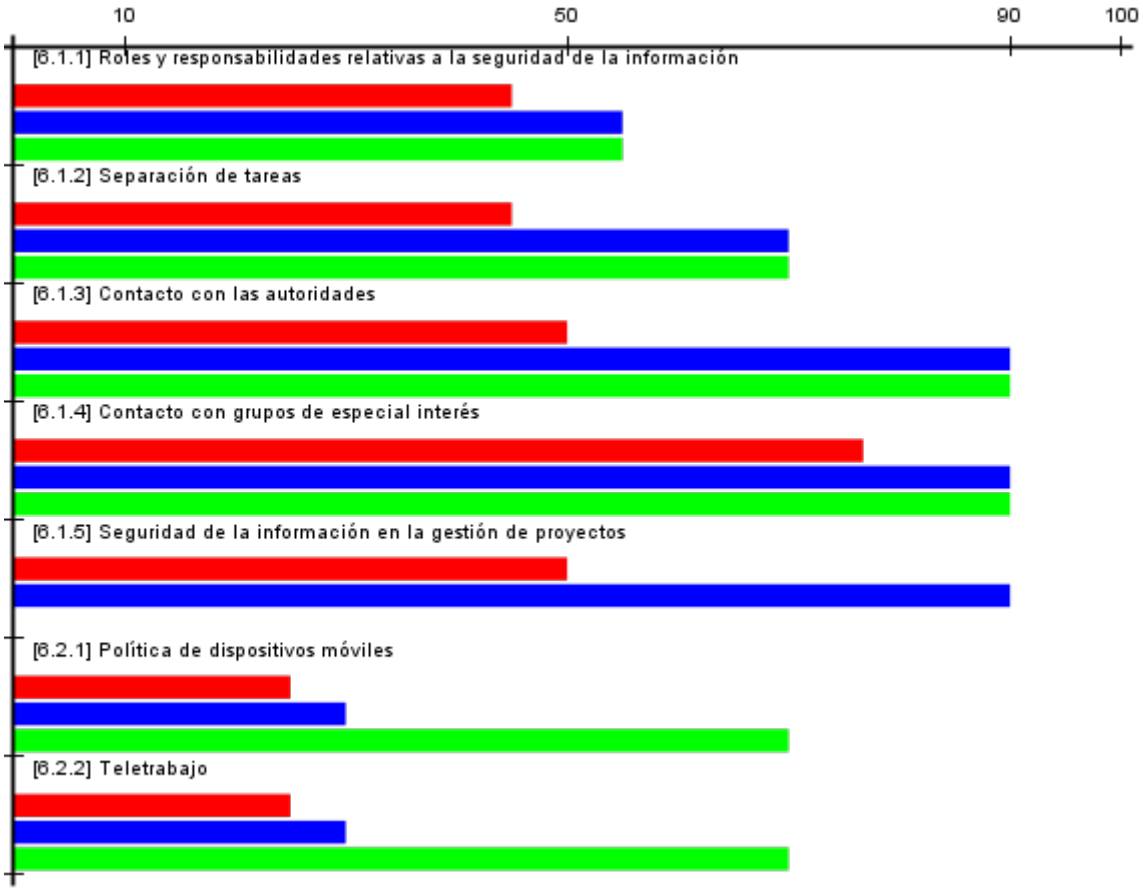
- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

[TEE] Tauler Edictes Electrònic

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{1,3}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{0,84}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,45}	{0,84}	{0,85}

4.3.7.2. Exemple d'anàlisi diferencial

[6] Organización de la seguridad de la información



[base] Base

control	[actual]	[objetivo]	[PILAR]
[6] Organización de la seguridad de la información	L0-L3	L1-L3	L2-L3
[6.1] Organización interna	L0-L3	L2-L3	L2-L3
[6.1.1] Roles y responsabilidades relativas a la seguridad de la información	L1-L3	L2-L3	L2-L3
[6.1.2] Separación de tareas	L0-L3	L2-L3	L2-L3
[6.1.3] Contacto con las autoridades	L2	L3	L3
[6.1.4] Contacto con grupos de especial interés	L2-L3	L3	L3
[6.1.5] Seguridad de la información en la gestión de proyectos	L2	L3	n.a.
[6.2] Dispositivos móviles y teletrabajo	L0-L2	L1-L2	L2-L3
[6.2.1] Política de dispositivos móviles	L0-L2	L1-L2	L2-L3
[6.2.2] Teletrabajo	L0-L2	L1-L2	L2-L3

La valoració està basada en el model de Maduresa de la Capacitat (CMM) que es pot consultar a l'Annex I.

5. Pla de Millora – Proposta de projectes

Avaluació dels projectes detectats a les fases anteriors i que s'hauran d'implementar per tal d'alinear-se amb el Pla Director, realitzant una quantificació econòmica i temporal.

S'ha calculat l'impacte de la "fase actual" el qual mostra l'estat real del risc del nostre sistema. En la nostra anàlisi s'han definit, utilitzant l'eina PILAR, una "fase objectiu" que serà l'estat al que voldrem arribar en un període entre 6 mesos i 1 any. Al final d'aquesta fase encara no haurem assolit els nivells de seguretat que determina la norma ISO/IEC 27002:2013 però ens hi trobarem més a prop.

Els nivells de seguretat que l'eina PILAR recomana per a la implantació de la norma es mostren en la fase anomenada "PILAR". La transició entre la fase "Objectiu" i la fase "PILAR" hauria de ser motiu una nova anàlisi de riscos realitzada a la fi de la "fase objectiu" i que permetés elaborar noves accions incloses en una revisió del Pla de Millora que hauria de durar aproximadament el mateix que per a la fase anterior, entre 6 mesos i 1 any. Així en un període de 2 anys assoliríem en ple compliment de la norma.

Es defineix un "Pla de Millora de la Seguretat" amb un conjunt d'actuacions de millora concretes estructurades en projectes i planificades en el temps que portin el nostre sistema als nivells de risc marcats a la "fase objectiu" i que permetin acostar els nostres sistemes a uns nivells que s'acostin, sinó poden ser assolits, als límits que marca el risc residual acceptats per la nostra organització.

5.1. Pla de millora de la seguretat

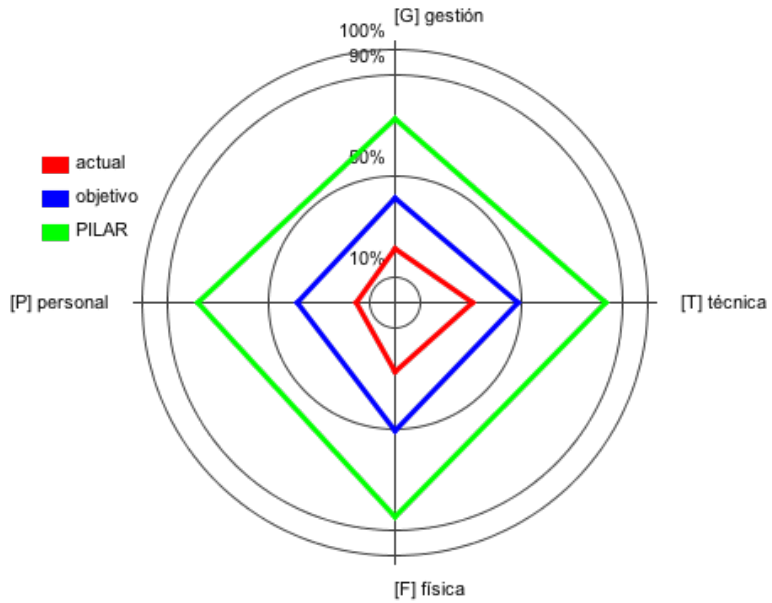
L'eina µPILAR utilitza per a la realització de l'anàlisi de riscos uns perfils de seguretat predefinits els quals utilitza per a associar un conjunt d'amenaces als actius definits segons les seves característiques. S'han avaluat 3 perfils en la realització de l'anàlisi de riscos: RD 1720 de protecció de dades de caràcter personal, SO/IEC 27002:2005 i ISO/IEC 27002:2013

El Pla de millora de la seguretat s'ha fet sobre l'avaluació del perfil ISO/IEC 27002:2013 i el seu objectiu és fer que l'Ajuntament de Fita Alta adopti unes actuacions de millora que el portin en l'avaluació del seu SGSI aplicat a la "Seu Electrònica" al compliment de la norma ISO/IEC 27001:2013 .

L'aprovació d'aquest Pla de Millora de la Seguretat, el seu desplegament en projectes i la seva temporalització correspon al Comitè de Seguretat.

La recomanació és que la implantació del Pla de Millora per a assolir els nivells de risc definits a la "fase objectiu" es faci en un any. Això ens acostarà als nivells de seguretat establerts per la norma ISO/IEC 27000 el qual és un objectiu estratègic de l'organització. Tot això sense oblidar que com administració pública es té l'obligació del compliment de les mesures de l'Esquema Nacional de Seguretat (RD 3/2010 de 8 de gener) que són similars a les que marca la norma ISO/IEC.

La millora dels nivells de seguretat s'ha de realitzar mitjançant un conjunt de projectes que recullin les accions de millora identificades a l'anàlisi de riscos realitzada. D'acord amb les salvaguardes indicades, en el termini de 12 mesos, s'aconsegueix fer un salt en la millora dels serveis tot i que encara es mantenen allunyats del mínims que marca la norma ISO/IEC tal i com es pot observar en la gràfica següent que ens ofereix l'eina PILAR.



5.1.1. Perfil de seguretat : ISO/IEC 27002:2013

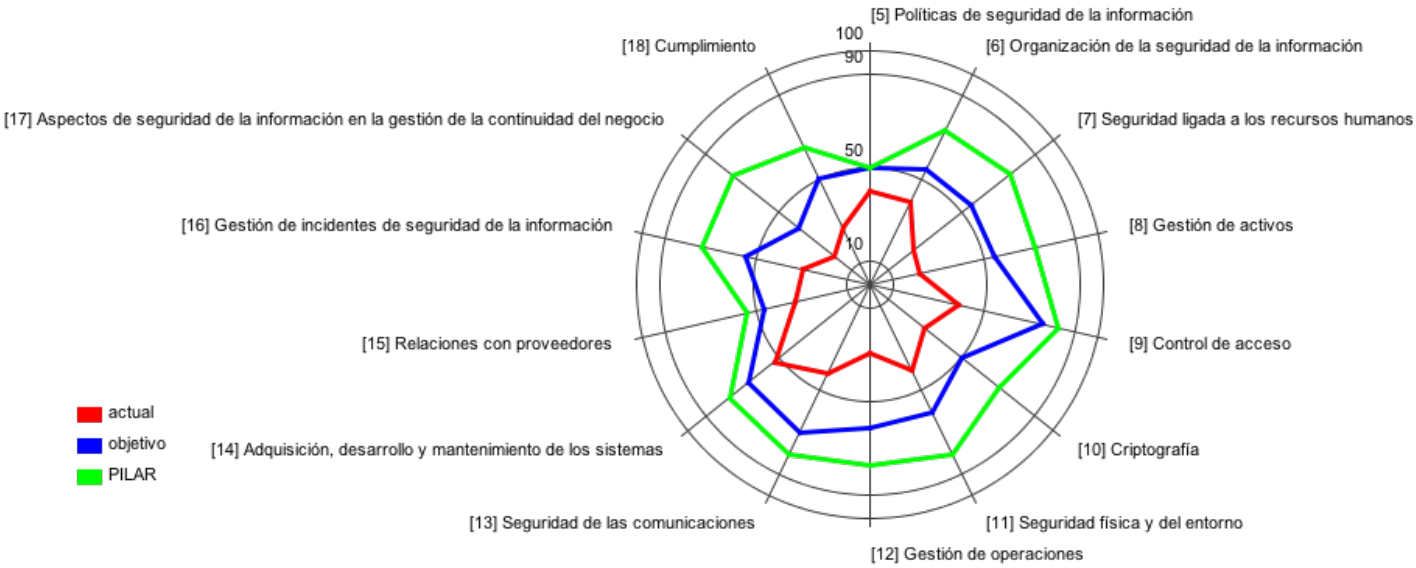
El programa PILAR permet veure el percentatge de mesures de seguretat aplicades a la "fase objectiu" i comparar-les amb els nivells mínims obligatoris definits per la norma i representats a la "fase PILAR".

[base] Base — Fuentes de información

rec...	control	...	f...	...	...	actual	objetivo	PILAR
	[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información					33%	56%	72%
2	[5] Políticas de seguridad de la información					40%	50%	50%
2	[5.1] Dirección de la gestión de la seguridad de la información					40%	50%	50%
5	[6] Organización de la seguridad de la información					39%	54%	73%
5	[6.1] Organización interna					53%	79%	76%
4	[6.2] Dispositivos móviles y teletrabajo					25%	30%	70%
6	[7] Seguridad ligada a los recursos humanos					23%	55%	76%
4	[7.1] Antes del empleo					21%	45%	80%
6	[7.2] Durante el empleo					31%	60%	68%
5	[7.3] Cese del empleo o cambio de puesto de trabajo					17%	60%	80%
6	[8] Gestión de activos					22%	55%	72%
5	[8.1] Responsabilidad sobre los activos					28%	62%	73%
5	[8.2] Clasificación de la información					12%	43%	73%
6	[8.3] Manipulación de los soportes					24%	59%	70%
8	[9] Control de acceso					39%	76%	83%
5	[9.1] Requisitos de negocio para el control de acceso					26%	65%	68%
7	[9.2] Gestión del acceso de usuario					39%	75%	84%
7	[9.3] Responsabilidades de usuario					50%	95%	95%
8	[9.4] Control de acceso al sistema y a las aplicaciones					39%	67%	83%
8	[10] Criptografía					30%	50%	70%
8	[10.1] Controles criptográficos					30%	50%	70%
8	[11] Seguridad física y del entorno					41%	60%	81%
7	[11.1] Áreas seguras					46%	62%	84%
8	[11.2] Equipos					36%	59%	77%
7	[12] Gestión de operaciones					29%	61%	78%
5	[12.1] Responsabilidades y procedimientos de operación					35%	51%	72%
7	[12.2] Protección contra el código malicioso					33%	70%	78%
5	[12.3] Copias de seguridad					42%	77%	83%
6	[12.4] Registro y monitorización					33%	61%	76%
7	[12.5] Control del software en explotación					30%	57%	71%
6	[12.6] Gestión de las vulnerabilidades técnicas					26%	62%	74%
5	[12.7] Consideraciones sobre la auditoría de los sistemas de información					5%	50%	90%
8	[13] Seguridad de las comunicaciones					42%	70%	81%
8	[13.1] Gestión de la seguridad de las redes					59%	80%	84%
5	[13.2] Transferencia de información					26%	60%	77%
6	[14] Adquisición, desarrollo y mantenimiento de los sistemas					53%	67%	77%
6	[14.1] Requisitos de seguridad de los sistemas de información					35%	59%	67%
4	[14.2] Seguridad en los procesos de desarrollo y soporte					34%	52%	75%
4	[14.3] Datos de prueba					90%	90%	90%
5	[15] Relaciones con proveedores					33%	47%	54%
3	[15.1] Seguridad de la información en las relaciones con proveedores					31%	44%	53%
5	[15.2] Gestión de servicios prestados por terceros					35%	50%	54%
5	[16] Gestión de incidentes de seguridad de la información					30%	55%	74%
5	[16.1] Gestión de incidentes de seguridad de la información y mejoras					30%	55%	74%
5	[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio					20%	39%	75%
5	[17.1] Continuidad de la seguridad de la información					3%	25%	76%
5	[17.2] Redundancia					36%	54%	75%
6	[18] Cumplimiento			...		27%	51%	65%
4	[18.1] Cumplimiento de los requisitos legales y contractuales			...		34%	56%	62%
6	[18.2] Revisiones de seguridad de la información					20%	46%	69%

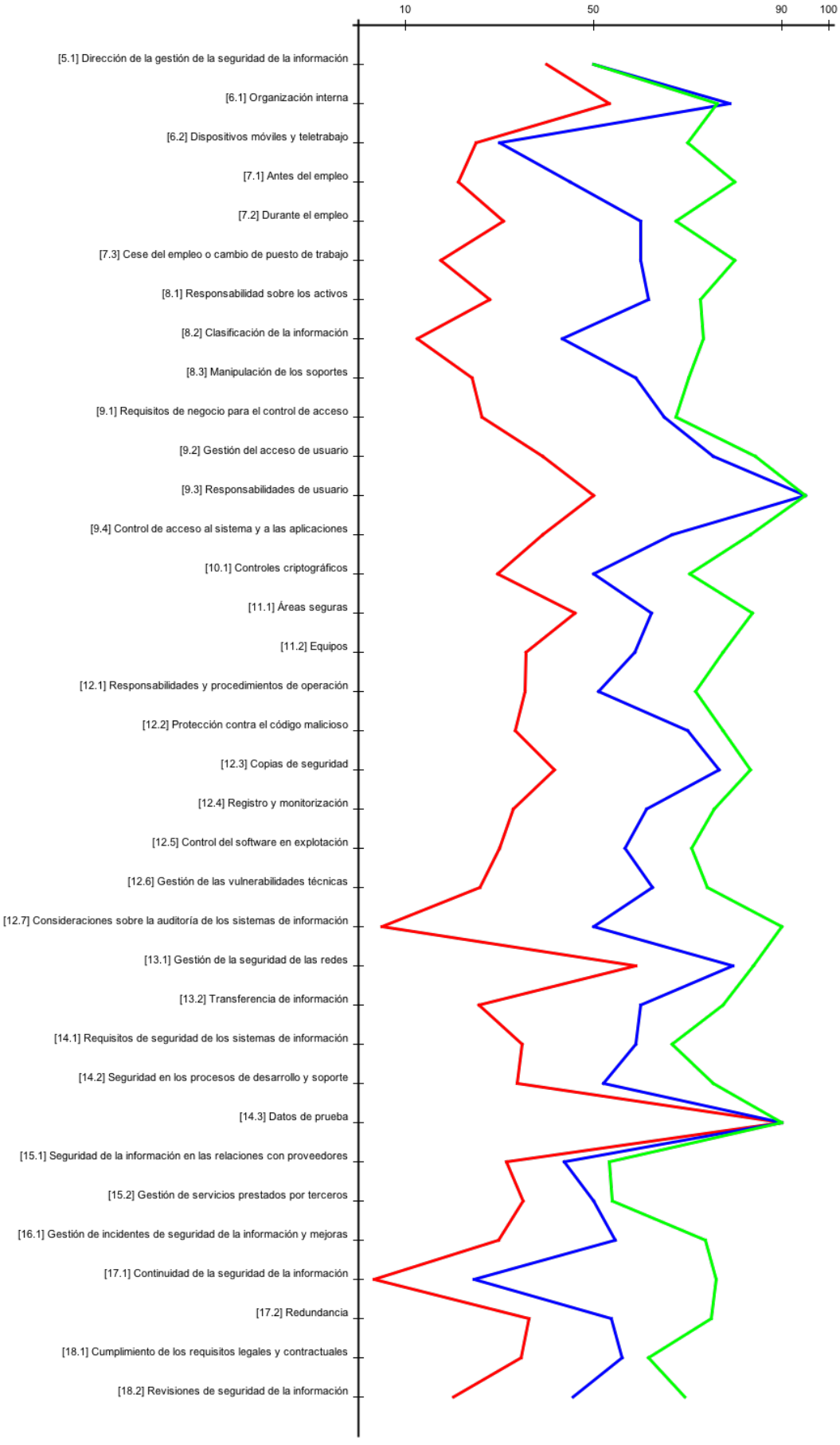
Es pot comprovar que per a tots els dominis de la norma, la fase objectiu, millora la situació. En tots els controls es realitza una aproximació als mínims que marca la norma preveient que en una segona fase es pugui arribar a assolir aquests objectius.

El gràfic següent ens permet veure quina és la situació de cada fase respecte als objectius a assolir per a cada domini de la norma ISO/IEC 27002:2013.



Les línies de color vermell marquen l'estat de la "fase actual" en els gràfics, les línies de color blau marquen l'estat al que s'arribaria a l'assolir la "fase objectiu" i les línies de color verd són les que indiquen els nivells mínims recomanats per la norma i que es marquen com a "fase PILAR".

L'eina PILAR també ens ofereix altres gràfics que permeten veure el grau de compliment per a cada objectiu de control de la norma i que es mostren a la pàgina següent. Com es comentava anteriorment, l'assoliment dels nivell de risc i compliment de la fase objectiu (de color blau) ens acostem als nivells requerits per la norma però es veu clarament que encara queda molt de camí per a recórrer i caldrà, com a mínim, un altre any per a poder arribar a nivells normatius.


10
50
90
100
[5.1] Dirección de la gestión de la seguridad de la información
[6.1] Organización interna
[6.2] Dispositivos móviles y teletrabajo
[7.1] Antes del empleo
[7.2] Durante el empleo
[7.3] Cese del empleo o cambio de puesto de trabajo
[8.1] Responsabilidad sobre los activos
[8.2] Clasificación de la información
[8.3] Manipulación de los soportes
[9.1] Requisitos de negocio para el control de acceso
[9.2] Gestión del acceso de usuario
[9.3] Responsabilidades de usuario
[9.4] Control de acceso al sistema y a las aplicaciones
[10.1] Controles criptográficos
[11.1] Áreas seguras
[11.2] Equipos
[12.1] Responsabilidades y procedimientos de operación
[12.2] Protección contra el código malicioso
[12.3] Copias de seguridad
[12.4] Registro y monitorización
[12.5] Control del software en explotación
[12.6] Gestión de las vulnerabilidades técnicas
[12.7] Consideraciones sobre la auditoría de los sistemas de información
[13.1] Gestión de la seguridad de las redes
[13.2] Transferencia de información
[14.1] Requisitos de seguridad de los sistemas de información
[14.2] Seguridad en los procesos de desarrollo y soporte
[14.3] Datos de prueba
[15.1] Seguridad de la información en las relaciones con proveedores
[15.2] Gestión de servicios prestados por terceros
[16.1] Gestión de incidentes de seguridad de la información y mejoras
[17.1] Continuidad de la seguridad de la información
[17.2] Redundancia
[18.1] Cumplimiento de los requisitos legales y contractuales
[18.2] Revisiones de seguridad de la información

5.2. Definició de projectes

S'ha fet una definició dels projectes necessaris per a solventar les deficiències detectades en el compliment dels requisits establerts per la norma ISO/IEC 27002:2013, a partir dels informes extrets per l'eina PILAR.

Cada projecte conté les actuacions de millora i tasques a realitzar i les salvaguardes sobre les que s'han d'aplicar.

Aquestes accions de millora es podrien haver agrupat seguint els 14 dominis que marca la norma i visualitzar d'aquesta forma les accions a realitzar per a donar compliment a cadascuna. Aquesta visió posa el focus en la norma i deixa de banda les especificitats que pugui tenir el nostre SGSI.

Una altra opció hagués estat agrupar el projectes en funció dels serveis que ofereix el nostre sistema i/o de les dimensions de seguretat que els hi són d'aplicació. Aquesta visió posa el focus en els serveis i deixa de banda les característiques generals que tot SGSI té amb independència dels seu serveis essencials.

S'ha optat per fer una agrupació diferent que posi juntes accions similars realitzades per controls de diferents dominis i amb independència de les dimensions de seguretat a les que hi apliqui, com per exemple l'elaboració de polítiques o procediments. Creiem que aquest plantejament posa el focus en el nostre SGSI, el domini "Seu Electrònica", de forma global i fa que les accions siguin més fàcils d'implantar i concretar en projectes. També és un enfocament que permet la adaptació del SGSI a noves etapes o cicles de millora i a l'ampliació dels seus serveis essencials.

Els diferents projectes identificats i que incorporen les actuacions de millora són:

- Desenvolupament del marc normatiu i procedimental de seguretat
- Control d'accés lògic
- Gestió de suports d'emmagatzemament
- Monitorització operativa de la seguretat
- Pla de continuïtat del negoci
- Gestió de la seguretat de la informació
- Formació i conscienciació en seguretat
- Ús de criptografia
- Enfortiment de les configuracions en els equips i les aplicacions
- Processos d'operació tècnica de la seguretat
- Aspectes jurídics relacionats amb la seguretat
- Protecció física de les infraestructures

L'agrupació en aquests projectes és basa en l'aprofitament de la realització d'auditories prèvies realitzades a l'Ajuntament de Fita Alta. La normativa estatal obliga a realitzar auditories de compliment de les mesures establertes al RD 1720/2007 de protecció de dades personals de forma bianual. Al 2013 també

es va realitzar una auditoria de compliment de les mesures de seguretat en l'àmbit de l'administració electrònica definides al RD 3/2010 que regula l'Esquema Nacional de Seguretat.

L'experiència en el desplegament de projectes anteriors fa que haguem triat l'agrupació descrita ja que inclou tant aspectes de protecció de dades personals com aspectes de compliment de mesures de seguretat i es pot aplicar perfectament al desplegament de la norma ISO/IEC 27000 i alhora seguir amb la mateixa línia de projectes desplegats fins a data d'avui.

Les salvaguardes contemplades en cada projecte són aquelles que estan per sota del nivell recomanat per la norma i marcats a la "fase PILAR" i estan extrets de l'informe de insuficiències (vulnerabilitats) de l'eina PILAR amb un nivell d'eficàcia inferior a L3 i que es poden consultar a l'Annex VIII.

5.2.1. Desenvolupament del marc normatiu i procedimental de seguretat

Consisteix en la formalització i documentació de les normes i procediments de seguretat necessaris per a implementar les mesures de seguretat seleccionades en la Declaració d'Aplicabilitat.
Les tasques a realitzar són l'elaboració i redacció de documents que permetin evidenciar la formalització de les mesures de seguretat i definir els requisits de seguretat i el desglossament de cada una de les activitats que componen un procediment amb els corresponents responsables.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
A. - 75 Accions	
Proteccions generals (4)	[H.IA] Identificación y autenticación [H.IA.1] Se dispone de normativa de identificación y autenticación
	[H.AC] Control de acceso lógico [H.AC.1] Se dispone de normativa para el control de accesos
	[H.VM] Gestión de vulnerabilidades [H.VM.6] Se dispone de procedimientos de reacción
	[H.AU] Registro y auditoría [H.AU.1.1] Se dispone de normativa acerca del registro de auditoria
Proteccions de la informació (4)	[D.2] Se dispone de un inventario de activos de información
	[D.3] Normativa [D.3.4] Se dispone de normativa de retención de datos
	[D.DS] Uso de firmas electrónicas [D.DS.1] Se dispone de normativa sobre firma electrónica
	[D.TS] Uso de servicios de fechado electrónico (time stamping) [D.TS.1] Se dispone de normativa de fechado electrónico
Gestió de claus	[K.comms] Gestión de claves de comunicaciones

ÀMBIT	SALVAGUARDES
A. - 75 Accions	
criptogràfiques (1)	[K.comms.1] Se dispone de normativa de gestión de claves
Proteccions dels serveis (8)	[S.1] Uso de los servicios [S.1.1] Se dispone de normativa relativa al uso de los servicios
	[COM.Internet] Navegación web [COM.Internet.1] Se dispone de normativa de uso
	[S.TW] Teletrabajo [S.TW.2] Se dispone de normativa de uso
	[S.2] Prestación de los servicios [S.2.1] Se dispone de un inventario de servicios
	[S.CM] Gestión de cambios (mejoras y sustituciones) [S.CM.1] Se dispone de normativa de control de cambios
	[S.2.a] Seguridad del comercio electrónico [S.2.a.2] Redacción y aprobación de un documento que consigne los términos acordados entre las partes
	[S.3] Servicios subcontratados [S.3.2] Contratos de prestación de servicios
Protecció de les aplicacions (9)	[SW.1] Se dispone de un inventario de aplicaciones (SW)
	[SW.2] Se dispone de normativa relativa a las aplicaciones (SW)
	[SW.3] Se dispone de procedimientos de uso de las aplicaciones
	[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)
	[SW.backup] Copias de seguridad (backup) (SW)
	[SW.start] Puesta en producción
	[SW.SC] Se aplican perfiles de seguridad
	[SW.op] Explotación / Producción [SW.op.1] Se dispone de normativa relativa al software en producción
	[SW.CM] Cambios (actualizaciones y mantenimiento) [SW.CM.1] Se dispone de una política
Protecció dels equips (10)	[HW.1] Se dispone de un inventario de equipos (HW)
	[HW.2] Se dispone de normativa sobre el uso correcto de los equipos
	[HW.3] Se dispone de procedimientos de uso del equipamiento
	[HW.SC] Se aplican perfiles de seguridad
	[HW.op] Operación [HW.op.1] Proceso de autorización de recursos para el tratamiento de la información
	[HW.CM] Cambios (actualizaciones y mantenimiento) [HW.CM.1] Se dispone de una política
	[HW.PCD] Informática móvil [HW.PCD.1] Se mantiene un inventario de equipos móviles con identificación del responsable de cada uno
	[HW.e] Maquinas virtuales [HW.e.1] Para la creación de nuevas máquinas virtuales se requiere autorización previa
	[HW.print] Reproducción de documentos

ÀMBIT	SALVAGUARDES
A. - 75 Accions	
	[HW.print.2] Asignación de cuentas de usuario
	[HW.h] Voz, facsímil y video [HW.h.1] Está prohibido establecer de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección
Protecció de les comunicacions (8)	[COM.1] Se dispone de un inventario de servicios de comunicación
	[COM.2] Se dispone de normativa sobre el uso correcto de las comunicaciones
	[COM.3] Se dispone de procedimientos de uso de las comunicaciones
	[COM.SC] Se aplican perfiles de seguridad
	[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados [COM.C.1] Se dispone de normativa relativa al uso de controles criptográficos
	[COM.op] Operación [COM.op.1.1] Se dispone de normativa de uso de los servicios de red
	[COM.CM] Cambios (actualizaciones y mantenimiento) [COM.CM.1] Se dispone de una política
	[COM.wifi] Seguridad Wireless (WiFi) [COM.wifi.1] Se requiere autorización prevla para desplegar puntos de acceso (AP)
Punts d'interconnexió (1)	[IP.1] Administración P.1.2] Se dispone de un inventario de conexiones autorizadas
Protecció dels suports d'informació (7)	[MP.1] Se dispone de normativa relativa a soportes de información
	[MP.2] Se dispone de procedimientos relativos a soportes de información
	[MP.3] Se dispone de un inventario de soportes
	[MP.7] Seguridad de los soportes fuera de las instalaciones [MP.7.4] Se dispone de normativa de uso de soportes fuera de las instalaciones
	[MP.IC] Protección criptográfica del contenido – A, C, H [MP.IC.1] Se dispone de normativa relativa a la protección criptográfica de los contenidos
	[MP.clean] Limpieza de contenidos [MP.clean.1] Se dispone de normativa que determina qué información debe ser eliminada de forma segura
	[MP.end] Destrucción de soportes [MP.end.1] Se dispone de normativa que determina qué soportes deben ser destruidos de forma segura
Elements auxiliars (1)	[AUX.1] Se dispone de un inventario de equipamiento auxiliar
Protecció de les instal·lacions (5)	[L.1] Se dispone de normativa de seguridad
	[L.2] Se dispone de un inventario de instalaciones
	[L.3] Entrada en servicio [L.3.1] Se dispone de normativa de entrada en servicio
	L.AC] Control de los accesos físicos

ÀMBIT	SALVAGUARDES
A. - 75 Accions	
	[L.cont] Continuidad de operaciones [L.cont.2] Se establece un protocolo de actuación en caso de contingencia
Gestió del personal (8)	[PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)
	[PS.2] Se dispone de procedimientos para la gestión de personal (en materia de seguridad)
	[PS.3] Relación de personal
	[H.ST] Segregación de tareas [H.ST.2] Se definen roles con autorización exclusiva para realizar tareas
	[PS.5] Puestos de trabajo [PS.5.5] Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
	[PS.6] Contratación – A [PS.6.1] Se dispone de normativa para la contratación de personal
	[PS.7] Cambio de puesto de trabajo
	[PS.c] Personal subcontratado
Gestió d'incidents (2)	[H.IR.1] Se dispone de normativa de actuación para la gestión de incidentes
	[H.IR.2] Se dispone de procedimientos para la gestión de incidentes [H.IR.2.1] Actuación frente a código dañino
Continuïtat del negoci (2)	[BC.1] Se dispone de normativa relativa a la continuidad del negocio
	[BC.2] El inventario se actualiza regularmente
Organització (5)	[G.1] Organización interna [G.1.2] Comité de seguridad de la información
	[G.2] Documentación técnica (componentes) [G.2.1] Documentación de los componentes del sistema
	[G.3] Documentación organizativa (normas y procedimientos) [G.3.2] Política de Seguridad de la Organización
	[RM] Gestión de riesgos – A, F [RM.1] Se dispone de normativa en materia de gestión de riesgos
	[G.plan] Planificación de la seguridad [G.plan.1] Se dispone de normativa de planificación (de seguridad)
Relacions externes (1)	[E.1] Acuerdos para intercambio de información y software

5.2.2. Control d'accés lògic

Consisteix en assegurar que només tenen accés als recursos aquelles persones prèviament autoritzades.

Les tasques a realitzar estan relacionades amb la gestió de la identitat i el control d'usuaris sobre els sistemes d'informació de l'Ajuntament.

L'abast afecta a l'àrea dels Sistemes d'Informació.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
B. - 5 Accions	
Proteccions generals (2)	[H.IA] Identificación y autenticación [H.IA.4] Gestión de la identificación y autenticación de usuario
	[H.AC] Control de acceso lógico [H.AC.8] Gestión de privilegios
Proteccions de la informació (1)	[D.5] Protección de la confidencialidad
Protecció dels equips (1)	[HW.e] Maquinas virtuales [HW.e.3] Se controla el acceso a las imágenes de las máquinas virtuales
Punts d'interconnexió (1)	[IP.2] Establecimiento de conexión [IP.2.1] Se identifican y autentican los usuarios antes de establecer el enlace [IP.2.3] El servidor se identifica y autentica antes de establecer el enlace
Protecció de les instal·lacions (1)	[L.6] Mecanismo de autenticación
Organització (1)	[G.2] Documentación técnica (componentes) [G.2.1.5] Documentación del control de aceso

5.2.3. Gestió de suports d'emmagatzemament

Consisteix en assegurar que la informació emmagatzemada gaudeix de mesures de protecció i es disposa dels procediments de tractament adequats segons el nivell de seguretat.

Les tasques a realitzar estan relacionades amb la gestió de suports i el cicle de vida de la informació: creació, etiquetatge, emmagatzematge, transport, difusió i destrucció.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
C. - 9 Accions	
Protecció dels equips (2)	[HW.op] Operación [HW.op.5] Seguridad de los equipos fuera de las instalaciones
	[HW.PCD] Informática móvil [HW.PCD.3] Cada equipo se marca con el nivel máximo de información que puede almacenar o procesar
Protecció dels suports d'informació (6)	[MP.4] Gestión de soportes [MP.4.1] Manejo [MP.4.2] Etiquetado [MP.4.3] Transporte de soportes
	[MP.6] Contenedores de seguridad
	[MP.7] Seguridad de los soportes fuera de las instalaciones [MP.7.3] Registro de entradas y salidas
	[MP.IC] Protección criptográfica del contenido [MP.IC.4] Se garantiza la integridad del contenido
	[MP.clean] Limpieza de contenidos [MP.clean.2] Se dispone de procedimientos para la limpieza de soportes
	[MP.end] Destrucción de soportes [MP.end.3] Se dispone de procedimientos para la destrucción de soportes
Adquisició / desenvolupament (1)	[NEW.MP] Soportes de Información: Adquisición

5.2.4. Monitorització operativa de la seguretat

Consisteix en establir les rutines d'operació de la seguretat que permetin la prevenció, detecció i correcció primerenca de possibles incidents de seguretat. Les tasques a realitzar estan relacionades amb l'anàlisi i la gestió de vulnerabilitats i la configuració de mesures preventives que evitin riscos.

L'abast afecta a l'àrea dels Sistemes d'Informació.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
D. - 18 Accions	
Proteccions generals (2)	[H.VM] Gestión de vulnerabilidades [H.VM.2] Mecanismos para estar informados de vulnerabilidades
	[H.AU] Registro y auditoría [H.AU.2] Herramientas
Proteccions dels serveis (7)	[COM.Internet] Navegación web [COM.Internet.2] Herramienta de monitorización del tráfico
	[S.2] Prestación de los servicios [S.cont] Aseguramiento de la disponibilidad
	[S.SC] Se aplican perfiles de seguridad
	[S.op] Explotación [S.op.1] Se realizan análisis periódicos de vulnerabilidades
	[S.CM] Gestión de cambios (mejoras y sustituciones) [S.CM.4] Se hace un seguimiento permanente (servicios externos)
	[S.2.a] Seguridad del comercio electrónico [S.2.a.6] Se dispone de un registro de actividades
	[S.3] Servicios subcontratados [S.3.3] Operación
Protecció dels equips (2)	[HW.cont] Aseguramiento de la disponibilidad [HW.cont.5] Se monitorizan fallos e incidentes
	[HW.print] Reproducción de documentos [HW.print.5] Se registra y se revisa la actividad de los dispositivos de reproducción
Protecció de les comunicacions (2)	[COM.cont] Aseguramiento de la disponibilidad [COM.cont.4] Se monitorizan enlaces y dispositivos de red
	[COM.op] Operación [COM.op.2.1] Se monitorizan los servicios de red
Punts d'interconnexió (1)	[IP.1] Administración [IP.1.3] Se realiza una monitorización continua de las conexiones autorizadas
Protecció dels suports d'informació (1)	[MP.cont] Aseguramiento de la disponibilidad
Elements auxiliars (1)	[AUX.cont] Aseguramiento de la disponibilidad
Gestió del personal (1)	[PS.cont] Aseguramiento de la disponibilidad [PS.cont.2] Se monitorizan continuamente los incidentes de disponibilidad de personal

ÀMBIT		SALVAGUARDES
D. - 18 Accions		
Gestió d'incidents	**(1)**	[H.IR.2] Se dispone de procedimientos para la gestión de incidentes [H.IR.2.d] Detección y reacción frente a actividades de robo de datos de carácter personal

5.2.5. Pla de continuïtat del negoci

Consisteix en dissenyar el pla de continuïtat de negoci que permeti disposar de mitjans alternatius en cas d'incidents greus.

Les tasques a realitzar estan relacionades amb l'anàlisi d'impacte del negoci, l'elaboració del pla de continuïtat de negoci i la possibilitat de disposar de mitjans i recursos alternatius en cas d'incidents greus.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
E. - 24 Accions	
Proteccions de la informació (1)	[D.backup] Copias de seguridad (backups) [D.backup.2] Protección de la disponibilidad de la información
Proteccions dels serveis (2)	[S.2] Prestación de los servicios [S.cont] Aseguramiento de la disponibilidad
	[S.3] Servicios subcontratados [S.3.6] Continuidad de operaciones
Protecció de les aplicacions (1)	[SW.backup] Copias de seguridad (backup) (SW)
Protecció dels equips (2)	[HW.cont] Aseguramiento de la disponibilidad [HW.cont.a] Alta disponibilitat
	[HW.e] Maquinas virtuales [HW.e.4] Se protegen las copias de seguridad de las imágenes de las máquinas virtuales
Protecció de les comunicacions (1)	[COM.cont] Aseguramiento de la disponibilidad [COM.cont.a] Redundancia
Punts d'interconnexió (1)	[IP.BS] Protección de los equipos de frontera [IP.BS.5] Se establece un plan de contingencia específico
Protecció dels suports d'informació (1)	[MP.cont] Aseguramiento de la disponibilidad
Elements auxiliars (4)	[AUX.cont] Aseguramiento de la disponibilidad
	[AUX.start] Instalación
	[AUX.power] Suministro eléctrico [AUX.power.6] Alimentación de respaldo
	[AUX.wires] Protección del cableado
Protecció de les instal·lacions (1)	[L.cont] Continuidad de operaciones [L.cont.3] Se dispone de instalaciones alternativas
Gestió del personal (1)	[PS.cont] Aseguramiento de la disponibilidad [PS.cont.3] Redundancia
Gestió d'incidents (1)	[H.IR.3] El personal designado cubre 24h 7 días de la semana
Continuïtat del negoci (3)	[BC.5] Reacción (gestión de crisis)

ÀMBIT	SALVAGUARDES
E. - 24 Accions	
	[BC.DRP] Plan de Recuperación de Desastres (DRP) [BC.DRP.5] Se dispone de un plan de recuperación
	[BC.7] Restitución (retorno a condiciones normales de trabajo)
Adquisició / desenvolupament (5)	[NEW.S] Servicios: Adquisición o desarrollo [NEW.S.2] Se establecen previamente los requisitos funcionales
	[NEW.SW] Aplicaciones: Adquisición o desarrollo [NEW.SW.1] Se establecen previamente los requisitos funcionales
	[NEW.HW] Equipos: Adquisición o desarrollo [NEW.HW.1] Se establecen previamente los requisitos funcionales
	[NEW.COM] Comunicaciones: Adquisición o contratación [NEW.COM.1] Se establecen previamente los requisitos funcionales
	[NEW.C] Productos certificados o acreditados

5.2.6. Gestió de la seguretat de la informació

Consisteix en determinar quines són les necessitats en matèria de seguretat mitjançant la realització d'una anàlisi de riscos i la implantació d'un pla de millora contínua.

Les tasques a realitzar estan relacionades amb l'anàlisi i la gestió del risc de l'Ajuntament.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT		SALVAGUARDES
F. - 10 Accions		
Proteccions generals	**(2)**	[H.AU] Registro y auditoría [H.AU.3] Información
		[S.3] Servicios subcontratados [S.3.1.4] Se identifican los riesgos derivados de depender de un proveedor externo
Elements auxiliars	**(1)**	[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos
Gestió d'incidents	**(2)**	[H.IR.5] Gestión del incidente [H.IR.5.4] Se planifica la implantación de medidas correctoras
		[H.IR.f] Se aprende de los incidentes
Continuïtat del negoci	**(1)**	[BC.BIA] Se ha realizado un análisis de impacto (BIA)
Organització	**(4)**	[G.1] Organización interna – A, F [G.1.3] Coordinación interna
		[RM] Gestión de riesgos – A, F [RM.3] Se dispone de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos
		[G.plan] Planificación de la seguridad [G.plan.2] Procedimientos de planificación (de seguridad)
		[G.exam] Inspecciones de seguridad

5.2.7. Formació i conscienciació en seguretat

Consisteix en capacitar i entrenar el personal per aconseguir que formin part activa de les mesures de protecció implantades.

Les tasques a realitzar estan relacionades amb la conscienciació, formació i entrenament al personal en matèria de seguretat de la informació, de manera que puguin identificar situacions de risc i notificar qualsevol sospita que suposi un incident potencial o real.

L'abast afecta a tot l'Ajuntament.
En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
G. - 11 Accions	
Proteccions de la informació (1)	[D.5.2] Limpieza de documentos publicados
Proteccions dels serveis (3)	[S.1] Uso de los servicios [S.1.3.4] Se forma a los usuarios en el uso de los servicios
	[S.TW] Teletrabajo [S.TW.3] Se forma a los usuarios en el uso de los servicios
	[S.op] Explotación [S.op.4] El personal recibe formación específica en configuración de servicios
Protecció dels equips (3)	[HW.op] Operación [HW.op.8] Formación del personal en configuración de equipos
	[HW.PCD] Informática móvil [HW.PCD.6] Se sigue un plan de concienciación sobre los riesgos y las medidas pertinentes
	[HW.h] Voz, facsímil y video [HW.h.3] Los usuarios están concienciados y reciben formación sobre el uso seguro de los sistemas y recursos disponibles
Protecció dels suports d'informació (1)	[MP.4] Gestión de soportes [MP.4.4] Formación del personal en gestión de soportes
Gestió del personal (1)	[PS.AT] Formación y concienciación
Gestió d'incidents (1)	[H.IR.e] Formación y concienciación [H.IR.e.2] Formación del personal en detección y gestión de incidentes
Continuïtat del negoci (1)	[BC.DRP] Plan de Recuperación de Desastres (DRP) [BC.DRP.6] Se ejecuta un plan de formación

5.2.8. Ús de criptografia

Consisteix en determinar les mesures de seguretat lògica a aplicar sobre suports d'informació per garantir la confidencialitat, integritat i autenticitat de les dades.

Les tasques a realitzar estan relacionades amb la implementació de certificats electrònics i la signatura electrònica.

L'abast afecta a l'àrea dels Sistemes d'Informació.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
H. - 10 Accions	
Proteccions de la informació (1)	[D.C] Cifrado de la información
Gestió de claus criptogràfiques (1)	[K.comms] Gestión de claves de comunicaciones [K.comms.4] Operación
Proteccions dels serveis (2)	[S.2.a] Seguridad del comercio electrónico [S.2.a.4] Implantación de mecanismos de autenticación de las partes
	[S.3] Servicios subcontratados [S.3.5] Autenticación del servidor – Criptografia: firma digital
Protecció dels equips (2)	[HW.7] Contenedores criptográficos (HW, HW virtual)
	[HW.PCD] Informática móvil [HW.PCD.8.5] Se han establecido los requisitos de cifrado
Protecció de les comunicacions (2)	[COM.aut] Autenticación del canal [COM.aut.4] Mecanismo de autenticación
	[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados [COM.C.4] Mecanismo de cifrado (secreto compartido o cifra simétrica)
Punts d'interconnexió (1)	[IP.2] Establecimiento de conexión [IP.2.3] El servidor se identifica y autentica antes de establecer el enlace
Protecció dels suports d'informació (1)	[MP.IC] Protección criptográfica del contenido [MP.IC.9] Mecanismo de cifrado

5.2.9. Enfortiment de les configuracions en els equips i les aplicacions

Consisteix en establir uns requisits tècnics previs a la posada en marxa d'aplicacions, equips o sistemes que garanteixin la seguretat per defecte i dotar de les mesures tècniques preventives als equips i aplicacions per evitar potencials incidents.

Les tasques a realitzar estan relacionades amb la implementació de mesures tècniques de seguretat i la configuració i ajust dels paràmetres de seguretat que enforteixin els equips i aplicacions, i així evitar determinats tipus d'amenaces que puguin afectar-los.

L'abast afecta a l'àrea dels Sistemes d'Informació.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
I. - 17 Accions	
Proteccions generals (1)	[H.tools] Herramientas de seguridad [H.tools.AV] Herramienta contra código dañino
Proteccions de la informació (5)	[D.I] Protección de la integridad
	[D.5.2] Limpieza de documentos publicados
	[D.DS] Uso de firmas electrónicas [D.DS.4] Se garantiza la eficacia probatoria de la firma
	[D.TS] Uso de servicios de fechado electrónico (time stamping) [D.TS.6] Mecanismo de fechado electrónico
	[S.TW] Teletrabajo [S.TW.6] Se dispone de procedimientos para gestión del teletrabajo
Protecció de les aplicacions (1)	[SW.op] Explotación / Producción [SW.op.6] Seguridad de las aplicaciones
Protecció dels equips (4)	[HW.op] Operación [HW.op.2] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico
	[HW.CM] Cambios (actualizaciones y mantenimiento) [HW.CM.a] Se planifica el cambio de forma que minimice la interrupción del servicio
	[HW.PCD] Informática móvil [HW.PCD.8.7] Se instala software antivirus y se mantiene actualizado
	[HW.h] Voz, facsímil y video [HW.h.6] Se previene el envío de documentos a números equivocados
Protecció de les comunicacions (3)	[COM.I] Protección de la integridad de los datos intercambiados

ÀMBIT	SALVAGUARDES
I. - 17 Accions	
	[COM.9] Se toman medidas frente a la inyección de información espuria
	[COM.wifi] Seguridad Wireless (WiFi) [COM.wifi.a] Se autentican los dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)
Punts d'interconnexió (3)	[IP.SPP] Tráfico: Intercambio de datos [IP.SPP.4] Se controla el tráfico entrante y saliente
	[IP.4] {xor} Arquitectura de protección: red local (LAN) [IP.4.2] Cortafuegos (control de sesión)
	[IP.BS] Protección de los equipos de frontera [IP.BS.3.2] Se verifica su configuración de seguridad

5.2.10. Processos d'operació tècnica de la seguretat

Consisteix en establir les rutines d'operació tècnica de la seguretat que permetin el manteniment tècnic, la gestió del canvi i la supervisió de les tasques de seguretat que es requereixen cada dia per garantir la seguretat dels sistemes d'informació.

Les tasques a realitzar estan relacionades amb el manteniment tècnic, la gestió del canvi i les tasques d'operació de la seguretat.

L'abast afecta a l'àrea dels Sistemes d'Informació.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
J. - 25 Accions	
Proteccions generals (6)	[H.AU] Registro y auditoría [H.AU.4] Actividades
	[S.start] Aceptación y puesta en operación
	[S.CM] Gestión de cambios (mejoras y sustituciones) [S.CM.e] Se actualizan todos los procedimientos de producción afectados
	[S.2.a] Seguridad del comercio electrónico [S.2.a.4] Implantación de mecanismos de autenticación de las partes
	[S.3] Servicios subcontratados [S.3.3] Operación
	[S.3] Servicios subcontratados [S.3.4] Gestión de cambios
Protecció de les aplicacions (2)	[SW.start] Puesta en producción
	[SW.CM] Cambios (actualizaciones y mantenimiento) [SW.CM.i] Se actualizan todos los procedimientos de producción afectados
Protecció dels equips (4)	[HW.start] Puesta en producción
	[HW.9] Instalación
	[HW.op] Operación [HW.op.4] Seguridad del equipamiento de oficina
	[HW.PCD] Informática móvil [HW.PCD.a] Gestión de incidentes en informática móvil
Protecció de les comunicacions (3)	[COM.start] Entrada en servicio
	[COM.CM] Cambios (actualizaciones y mantenimiento) [COM.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio
	[COM.wifi] Seguridad Wireless (WiFi) [COM.wifi.8] Se comprueban periódicamente los puntos de acceso (mediante broadcast o herramientas)

ÀMBIT	SALVAGUARDES
J. - 25 Accions	
Punts d'interconnexió (1)	[IP.2] Establecimiento de conexión [IP.2.3] El servidor se identifica y autentica antes de establecer el enlace
Protecció dels suports d'informació (1)	[MP.5] Se controla la conexión de dispositivos removibles
Gestió del personal (1)	[PS.9] Procedimientos de prevención y reacción [PS.9.1] frente a software dañino
Gestió d'incidents (3)	[H.IR.5] Gestión del incidente [H.IR.5.3] Se analiza el impacto del incidente
	[H.IR.a] Comunicación de los fallos del software
	[H.IR.c] Los fallos y las medidas correctoras se registran y se revisan
Adquisició / desenvolupament (4)	[NEW.S] Servicios: Adquisición o desarrollo [NEW.S.4] Se identifican los requisitos técnicos de seguridad
	[NEW.SW] Aplicaciones: Adquisición o desarrollo [NEW.SW.3] Se identifican los requisitos técnicos de seguridad
	[NEW.HW] Equipos: Adquisición o desarrollo [NEW.HW.3] Se identifican los requisitos técnicos de seguridad
	[NEW.COM] Comunicaciones: Adquisición o contratación [NEW.COM.5] Se identifican los requisitos técnicos de seguridad

5.2.11. Aspectes jurídics relacionats amb la seguretat

Consisteix en assegurar que les clàusules contractuals signades amb tercers garanteixin la cobertura jurídica necessària i contemplin els acords de nivell de servei que satisfan els requisits de seguretat establerts.

Les tasques a realitzar estan relacionades amb l'elaboració de clàusules legals en contractes de serveis externs i amb l'especificació de les activitats de seguiment i monitorització del compliment d'aquests contractes d'acord amb els nivells de servei pactats.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
K. - 8 Accions	
Proteccions dels serveis (2)	[S.2.a] Seguridad del comercio electrónico [S.2.a.2] Redacción y aprobación de un documento que consigne los términos acordados entre las partes
	[S.3] Servicios subcontratados [S.3.2] Contratos de prestación de servicios
Protecció de les aplicacions (1)	[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)
Protecció de les instal·lacions (1)	[L.b] Protección frente a desastres [L.b.8] Seguros
Adquisició / desenvolupament (4)	[NEW.S] Servicios: Adquisición o desarrollo [NEW.S.3] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
	[NEW.SW] Aplicaciones: Adquisición o desarrollo [NEW.SW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
	[NEW.HW] Equipos: Adquisición o desarrollo [NEW.HW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
	[NEW.COM] Comunicaciones: Adquisición o contratación [NEW.COM.4] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio

5.2.12. Protecció física de les infraestructures

Consisteix en determinar les mesures de seguretat física a aplicar a edificis, sales, persones i suports per garantir la seva correcta custòdia.

Les tasques a realitzar estan relacionades amb la implementació de mesures de seguretat físiques i lògiques de seguretat aplicable a cada tipus de recurs.

L'abast afecta a tot l'Ajuntament.

En la següent taula s'indiquen sobre quines salvaguardes incideix directament aquest projecte:

ÀMBIT	SALVAGUARDES
L. - 8 Accions	
Protecció dels equips (1)	[HW.op] Operación [HW.op.3] Protección física de los equipos
Protecció de les instal·lacions (7)	[L.3] Entrada en servicio [L.3.5] Plan de Protección
	[L.design] Diseño
	[L.depth] Defensa en profundidad
	L.AC] Control de los accesos físicos
	[L.8] Protección del perímetro
	[L.9] Vigilancia
	[L.b] Protección frente a desastres [L.b.2] Protección frente a incendios

5.3. Temporalització de projectes

Un cop s'han agrupat les accions proposades per l'eina Pilar en projectes cal fer una priorització/temporalització per a realitzar-les en un període de 12 mesos. El resultat obtingut són 12 projectes que aglutinen 220 accions que estan basades en les salvaguardes recomanades per l'eina PILAR.

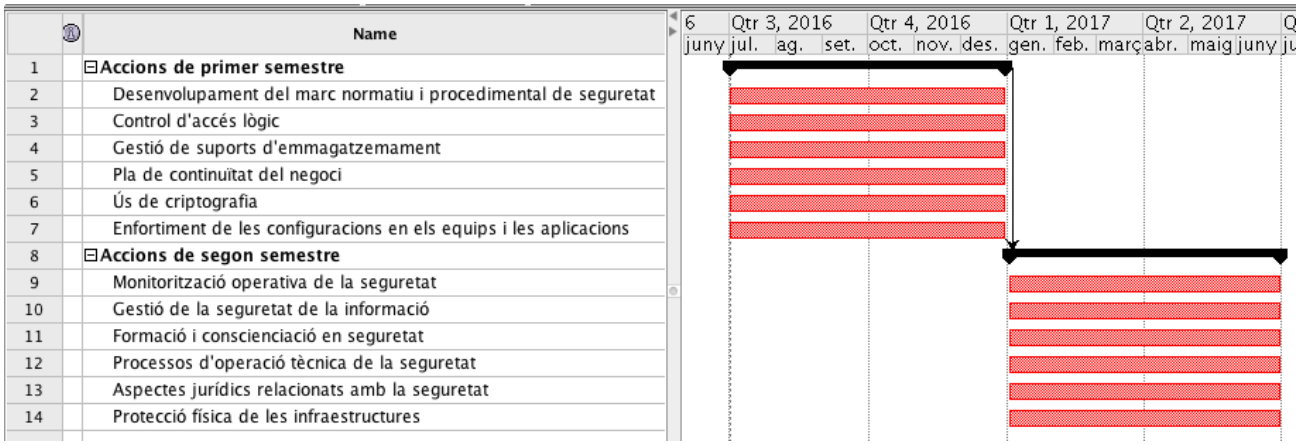
Donada la gran quantitat de projectes i accions a realitzar es fa una proposta dels que s'haurien d'iniciar en el primer semestre i els que es s'haurien d'iniciar en el segon amb l'objectiu que totes les seves respectives accions estiguin finalitzades un any després d'iniciar-se aquest Pla de Projectes.

Es proposa iniciar el primer semestre uns projectes que sumin aproximadament 2/3 de les accions previstes i durant el segon semestre iniciar la resta de projectes que donin compliment al 1/3 de les accions restants.

S'ha de tenir en compte que a la fase d'anàlisi de riscos anterior es van detectar **2** valoracions "**Crítiques**" que afectaven la Integritat i l'Autenticitat al servei de pagament on-line.

Això fa que haguem de contemplar dintre de les primeres accions de millora les relacionades amb la minimització dels riscs associats amb **l'autenticació** i la **integritat** dels **Pagaments On-Line**.

En el cas de l'autenticació cal parar atenció a la gestió de les credencials d'autenticació i les dades de configuració i gestió interna del servei. En el cas de la integritat les mesures faran referència a la gestió de la informació (fitxers de dades, còpies de seguretat, dades de configuració i gestió, aplicacions de gestió, ..) així com dels seus suports (emmagatzemament en xarxa, discos físics i virtuals).

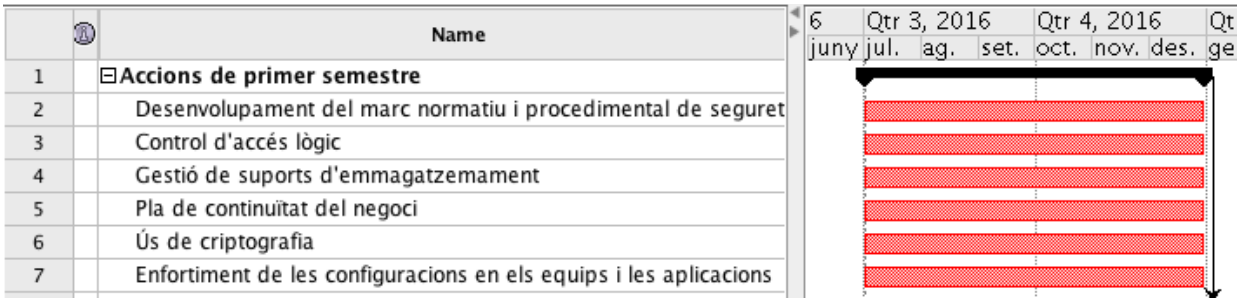


S'adjunta gràfica de temporalització dels projectes abans de fer un estudi més acurat de les tasques a realitzar per a cadascun d'ells.

5.3.1. Projectes a realitzar el primer semestre

Els projectes considerats per a iniciar durant els 6 primers mesos d'aplicació del Pla de Millora que es materialitza en aquest Pla de Projectes són:

PROJECTES A REALITZAR EL PRIMER SEMESTRE	ACCIONS
Desenvolupament del marc normatiu i procedimental de seguretat	75
Control d'accés lògic *	5
Gestió de suports d'emmagatzemament *	9
Pla de continuïtat del negoci *	24
Ús de criptografia *	10
Enfortiment de les configuracions en els equips i les aplicacions	17
Total accions	**140**



Els projectes marcats amb * són els que estan directament relacionats amb l'objectiu de reduir els riscos que afectaven la Integritat i l'Autenticitat al servei de pagament on-line.

Els aspectes relacionats amb les credencials d'autenticació és treballen fonamentalment amb el projecte de "Control d'accés lògic" i es complementen pel que fa a la configuració i gestió interna del servei amb el projeces de "Ús de criptografia". Són uns projectes d'àmbit intern del Servei de Sistemes d'Informació.

Els aspectes relacionats amb la integritat de les dades i els seus suports, es treballen amb els projectes de "Pla de continuïtat del negoci" i "Gestió de suports d'emmagatzemament". Aquests dos projectes són d'àmbit transversal a tota l'organització.

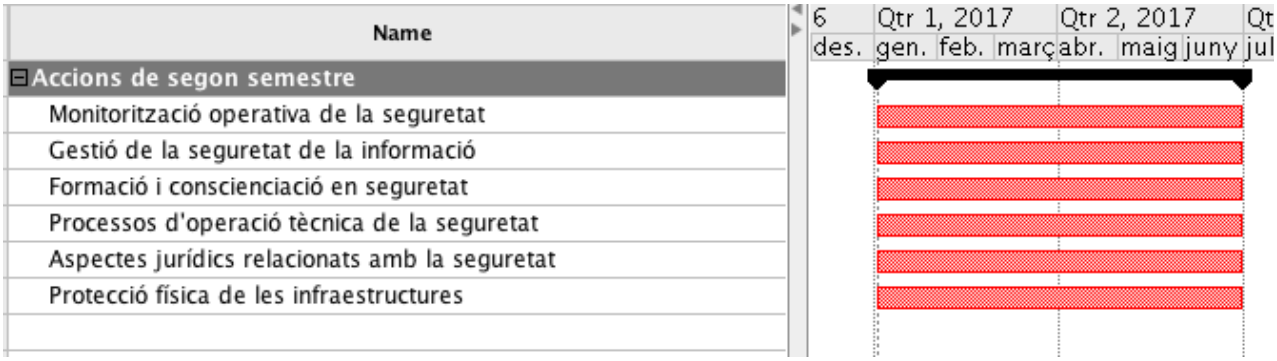
Aquests 4 projectes s'inicien en aquest primer semestre amb l'objectiu de minimitzar les principals amenaces detectades a l'anàlisi de riscos. Tots ells sumen 48 de les 140 accions contemplades el primer semestre.

El projecte "Enfortiment de les configuracions en els equips i les aplicacions" ha estat triat ja que moltes de les aplicacions de les accions proposades en els 4 projectes anteriors s'han de derivar en la implantació d'accions concretes en els nostres equips i aplicacions que es porten a la pràctica en les accions contemplades en aquest projecte. És el complement ideal per a complementar les accions anteriors alhora que produeix una millora general que impacta sobre tota l'organització. És un projecte d'àmbit intern del Servei de Sistemes d'Informació.

Per a finalitzar s'ha triat el projecte "Desenvolupament del marc normatiu i procedimental de seguretat". Aquest projecte contempla la definició de totes les polítiques, normes i procediments que tenen relació amb el nostre sistema de gestió de la seguretat. S'ha detectat una mancança generalitzada pel que fa la l'elaboració i difusió de les normes de seguretat que generen molts incompliments de la norma. Molts d'aquestes incompliments estan produïts no pas per accions o procediments incorrectes sinó pel fet de realitzar-los sense haver estat documentats i aprovats. Així que aquests és el primer pas que cal realitzar. La materialització de les accions d'aquest projecte implicarà una millora molt important de l'avaluació del nivell de maduresa de les nostres salvaguardes. És un projecte d'àmbit transversal a tota l'organització.

5.3.2. Projectes a realitzar el segon semestre

PROJECTES A REALITZAR EL SEGON SEMESTRE	ACCIONS
Monitorització operativa de la seguretat	18
Gestió de la seguretat de la informació	10
Formació i conscienciació en seguretat	11
Processos d'operació tècnica de la seguretat	25
Aspectes jurídics relacionats amb la seguretat	8
Protecció física de les infraestructures	8
Total accions	**80**



Els projectes del primer semestre iniciaven les accions més prioritàries per a corregir l'impacte dels riscos amb valoració crítica i s'afrontava el desenvolupament del marc normatiu. Durant el segon semestre i amb la majoria dels projectes del primer semestres finalitzats abordarem la resta d'accions que cal implantar per a que el nostre SGSI redueixi el seu llindar de risc. Aquest segon semestre només s'inicien 1/3 de les accions a realitzar ja que es contempla la possibilitat que encara no hagin acabat tots els projectes iniciats al primer semestre.

El projecte "Monitorització operativa de la seguretat" implantarà les mesures necessàries per a monitoritzar en tot moment el nostre SGSI i fer habilitat la prevenció, detecció i correcció primerenca de possibles incidents de seguretat. És un projecte d'àmbit intern del Servei de Sistemes d'Informació.

El projecte "Processos d'operació tècnica de la seguretat" establirà les rutines d'operació tècnica del manteniment, la gestió del canvi i supervisió de les tasques de seguretat diàries. És un projecte d'àmbit intern del Servei de Sistemes d'Informació.

El projecte "Gestió de la seguretat de la informació" té la finalitat de la implantació i posta en marxa del SGSI com un sistema de millora contínua basada en l'anàlisi i la gestió del risc. És un projecte d'àmbit transversal a tota l'organització i és el que té més pes de tots els de la segona fase.

El projecte "Formació i conscienciació en seguretat" vol assolir que tots el personal de l'organització sigui una part activa de les mesures de seguretat implantades. És un projecte d'àmbit transversal a tota l'organització i s'ha de basar en la conscienciació i la formació.

El dos projectes restants, "Aspectes jurídics relacionats amb la seguretat" i "Protecció física de les infraestructures" fan el tancament dels aspectes de la seguretat que faltava abordar: la cobertura jurídica i els acords de nivells de servei necessaris per a assolir els requisits de seguretat establerts i l'aplicació de mesures de seguretat física a edificis, sales, persones i suports.

La finalització d'aquests projectes suposaria la finalització de la implantació de les mesures contemplades a la "Fase Objectiu". En aquest moment i seguint el cicle de millora contínua, correspondria iniciar una nova anàlisi de riscos i sobre aquesta realitzar un pla de projectes per a la implantació de les mesures que ens permetin arribar als nivells de risc proposats per la norma ISO/IEC 27001:2013 i així successivament any rere any millorant el nostre SGSI i mantenint tots els objectius i controls dintres dels nivell del risc residual acceptats per la nostra organització.

5.3.3. Valoració econòmica del Pla de Projectes

La valoració econòmica del projecte necessitaria d'una banda el refinament que resta pendents de les activitats més detallades dels projectes i les dedicacions parcials per a cada projecte dels diferents perfils d'empleat de l'organització i de la realització d'una estimació de costos. El cost total de la implantació serà la suma dels costos de tots els projectes.

Es podria fer servir la taula següent de tarifes/jornada per a cada perfil considerant una dedicació del 100% :

Personal directiu	200 euros / jornada
Càrrecs intermedis, cap de seguretat, caps de departament o servei	120 euros / jornada
Tècnics de seguretat i de TI	90 euros / jornada
Operadors de seguretat i personal de l'Ajuntament	60 euros / jornada

Tenint el compte que cada projecte estaria dividit en fases es calcularia el cost de cada fase, per exemple, omplint la taula següent:

Perfil	**Nombre de Jornades**	**Activitats**
Director	1 jornada	Reunió inici projecte
Cap de seguretat	1 jornada	Reunió inici projecte
Tècnic de TI	1 jornada	Reunió inici projecte

Per a omplir la taula següent amb la informació recollida per a cada fase per a la realització del càlcul del cost total del projecte (com per exemple):

Durada	3 mesos
Dedicacions	Director : 3,5 jornades Cap de seguretat: 2,5 x 3 jornades Tècnic de TI : 15,5 jornades
Costos	200x3,5 + 120x2,5x3 + 90x15,5 = **2.995**

La suma de tots els projectes ens donaria una taula similar amb el cost i dedicació de tot el projecte.

No s'ha realitzat el càlcul detallat dels costos del projecte ja que no s'ha desenvolupat en la realització d'aquest lliurament les fases que tindria cadascun dels projectes identificats.

5.3.4. Priorització de les accions dels projectes

Ara caldria desglossar els projectes en subprojectes i establir una priorització entre ells. La priorització d'aquests subprojectes realitzarà accedint a l'apartat de valoracions de les salvaguardes i observant quins són els grups més recomanats per l'eina PILAR.

Les valoracions de les salvaguardes a l'eina PILAR segueixen un codi de colors que indiquen el seu grau de compliment de la norma avaluada.

- gris : la salvaguarda NO és aplicable
- vermell: la maduresa actual està molt per sota de l'objectiu (fase PILAR)
- groc : la maduresa actual està per sota de l'objectiu (fase PILAR)
- verd : la maduresa actual està a l'alçada de l'objectiu (fase PILAR)
- blau : la maduresa actual està per sobre de l'objectiu (fase PILAR)

Efectivitat	CMM	Significat
0%	L0	Inexistent
10%	L1	Inicial / Ad-hoc
50%	L2	Repetible, però intuïtiu
90%	L3	Definit
95%	L4	Gestionat i mesurable
100%	L5	Optimitzat

Les valoracions fetes a l'eina PILAR estan fetes sobre el model de Maduresa de la Capacitat (CMM) que es pot consultar a l'Annex I.

Les salvaguardes tenen pesos diferents que li donen una importància major a una que a una altra. L'eina PILAR les identifica a l'aplicació com a paraigües de colors.

Peso relativo

	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
	aseguramiento: componentes certificados	

La recomanació per a la priorització de les primeres accions a realitzar dintre dels projectes és seguir el criteri numèric del camp recomanació i començar per les que tenen un valor mes alt. Normalment aquestes seran les que tenen una

valoració L0 i una recomanació de PILAR més alta i és molt probable tinguin un color vermell. La Salvaguarda amb més pes dintre del mateix grup la trobarem marcada amb el paraigua de color vermell.

[base] Base | Fuentes de información

recomendación	control	d...	fu...	a...	co...	actual	objeti...	PILAR
4	[10.1.1] Política de uso de los controles criptográficos					L0-L2	L2	L2-L3
8	[10.1.2] Gestión de claves					L0-L3	L1-L3	L2-L5
8	[K] Gestión de claves criptográficas			...		L0-L3	L1-L3	L2-L5
8	[K.comms] Gestión de claves de comunicaciones					L0-L3	L1-L3	L2-L5
3	[K.comms.1] Se dispone de normativa de gestión de claves					L0	L2	L3
3	[K.comms.2] Se dispone de procedimientos de gestión de claves					L0	L1	L3
3	[K.comms.3] Se identifica la persona responsable de cada clave					L1	L2	L3
6	[K.comms.4] Operación					L2	L3	L3-L4
8	[K.comms.5] Las claves se generan en un entorno separado del de explotación					L3	L3	L5
5	[K.comms.6] {xor} Generación de claves					L3	L3	L3
8	[K.comms.7] {xor} Distribución de claves					L2	L3	L5
7	[K.comms.8] {xor} Almacenamiento de las claves					L1	L2	L4
5	[K.comms.9] Las claves se destruyen de forma segura					L0	L2	L3
6	[K.comms.a] Se retienen copias de las claves					L0	L1	L2-L4
	[K.509] Gestión de certificados					L1-L3	L2-L3	n.a.
8	[11] Seguridad física y del entorno					L0-L3	L0-L3	L2-L5

Després de les que tenen valoració L0 donaríem prioritat a les que tenen prioritat L1 i tenen una recomanació de PILAR més alta. I així successivament.

En aquest "Pla de Projectes" no arribarem a aquest nivell de detall per a cada projecte. Això correspondria al desplegament individual de cadascun dels projectes identificats. Ens limitem a donar els criteris de priorització que utilitzaríem per al desplegament de les tasques i a especificar els períodes d'execució en una planificació global de 12 mesos.

5.4. Conclusions – Resum executiu

Els nivells de seguretat que l'eina PILAR recomana per a la implantació de la norma es mostren en la fase anomenada "PILAR". La transició entre la "fase objectiu" i la "fase PILAR" hauria de ser motiu una nova anàlisi de riscos realitzada a la fi de la "fase objectiu" i que permetés elaborar noves accions incloses en una revisió del Pla de Millora que hauria de durar aproximadament el mateix que per a la fase anterior, entre 6 mesos i 1 any. Així en un període de 2 anys assoliríem en ple compliment de la norma.

La recomanació és que la implantació del Pla de Millora per a assolir els nivells de risc definits a la "fase objectiu" es faci en un any. Això ens acostarà als nivells de seguretat establerts per la norma ISO/IEC 27000 el qual és un objectiu estratègic de l'organització. Tot això sense oblidar que com administració pública es té l'obligació del compliment de les mesures de l'Esquema Nacional de Seguretat (RD 3/2010 de 8 de gener) que són similars a les que marca la norma ISO/IEC.

6. Informe d'Auditoria

L'Ajuntament de Fita Alta, després d'haver realitzat en un any tots els projectes definits al "Pla de projectes" vol realitzar una auditoria sobre el compliment de l'estàndard ISO/IEC 27002:2013 per a avaluar si ha millorar l'efectivitat de les mesures i en el compliment de les "bones pràctiques" en matèria de seguretat.

Aquesta auditoria no és una Auditoria de Certificació del compliment de la norma ISO/IEC 27001:2013 sinó una Auditoria d'avaluació de l'estat de la maduresa del SGSI de l'Ajuntament de Fita Alta utilitzant com a referència el catàleg de controls de la Norma ISO/IEC 27002:2013.

En aquest estadi del procés d'implantació, el SGSI de l'Ajuntament de Fita Alta encara no està prou madur per a donar-lo per a implantat i plantejar-se la certificació de la norma i la realització d'una auditoria de certificació. És aquest el motiu pel qual es vol realitzar una auditoria de maduresa dels controls de la norma i poder fer una avaluació objectiva sobre si la realització dels projectes ha assolit els objectius a nivell de millora en el compliment normatiu.

6.1. Objectiu de l'auditoria

L'objectiu de l'auditoria és avaluar la maduresa de la seguretat del SGSI de l'Ajuntament de Fita Alta pel que fa als diferents dominis de control plantejat per la ISO/IEC 27002:2013 després d'un any de l'inici de la implantació del sistema de seguretat i a la finalització de l'execució del Pla de Projectes.

6.2. Abast

L'auditoria té com a abast el SGSI implantat a l'Ajuntament de Fita Alta en la seva totalitat i la seva aplicació sobre els 14 dominis i 35 objectius de control de la norma ISO/IEC 27002:2013 contemplats en la declaració d'aplicabilitat del SGSI.

6.3. Metodologia utilitzada

La metodologia utilitzada serà la realització d'una "**Auditoria interna** o de **primera part**" ja que l'Ajuntament de Fita Alta és l'organització "Client" que encomana l'auditoria i alhora l'organització "Auditada". Aquest tipus d'auditoria s'acostuma a utilitzar per a detectar punts de millora en el fet auditat i serveix com a autoavaluació prèvia a altres tipus d'auditoria com podria ser una auditoria de certificació.

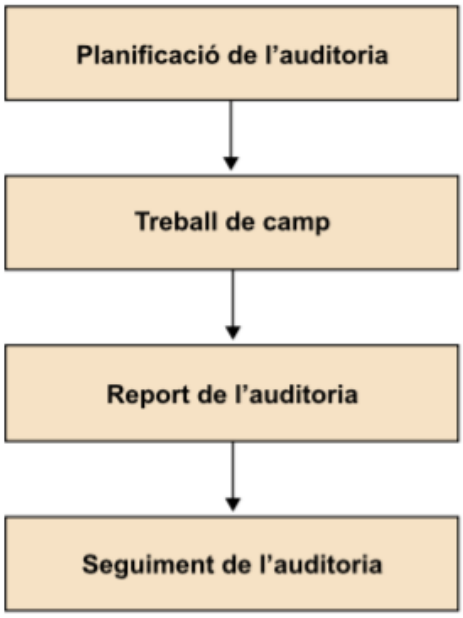
L'auditoria pot ser realitzada per un equip auditor propi o bé un d'extern però sempre designat per l'Ajuntament de Fita Alta que és el destinatari final dels resultats de l'auditoria.

En el cas que ens ocupa s'ha decidit realitzar l'auditoria amb personal intern de l'organització i on l'Auditor en cap és el "Responsable de seguretat" de l'Ajuntament de Fita Alta. L'auditor en cap podrà requerir de l'assistència de

tècnics municipals com a Experts Tècnics en les tasques que consideri convenients. Si es considerés interessant o necessari per a algun apartat concret també es podria requerir l'assessorament d'algun "Expert Tècnic extern" el qual actuaria sota la direcció de l'auditor en cap.

6.4. Procés d'auditoria

L'auditoria és realitzarà seguint un procés dividit en quatre fases:



Fases generals d'una auditoria

6.4.1. Planificació de l'auditoria

Inclou totes les activitats necessàries per a dotar l'auditoria d'un marc de treball, els recursos necessaris i els objectius que s'han de complir.
En aquesta fase s'han de realitzar les tasques següents:

- Designar l'equip auditor : en aquest cas només hi haurà un auditor que tindrà el càrrec d'auditor en cap i que li correspondrà al Cap de Seguretat de l'Ajuntament de Fita Alta.
- Definir l'abast i objectius de l'auditoria: detallats als punts 2 i 3 d'aquest document.
- Recopilar el material de camp per a la seva anàlisi posterior: en aquest cas i atès que es un estudi teòric en el marc del Treball de Fi de Màster (TFM en endavant) no ens podem basar en material de camp real.
  Utilitzarem el material generat en les fases anteriors i suposarem l'existència de documents i registres del SGSI si en la fase de planificació i realització dels projectes així es va especificar.
- Elaborar un Pla d'Auditoria: de forma que els seus criteris d'execució estiguin alineats amb els objectius i abast de l'auditoria.
  En aquest cas no elaborarem cap Pla d'Auditoria ja que el que es demana que es realitzi en l'àmbit del TFM és l'informe d'auditoria. L´únic que podem considerar inclòs en el Pla d'Auditoria és l'avaluació del nivell de maduresa dels controls de la norma. Tot i no elaborar-lo formalment, en tot moment es donarà per suposat que el Pla d'Auditoria existeix i

que totes les accions realitzades s'han fet d'acord a les seves indicacions.

6.4.2. Treball de camp

És l'activitat principal de l'auditoria i consisteix en l'execució del Pla d'Auditoria fent les diferents proves d'auditoria que buscaran comprovar la forma en que es compleixen els criteris.
En el cas que ens ocupa ens limitarem a realitzar una única prova consistent en l'avaluació del nivell de maduresa dels diferents controls de la norma ISO/IEC 27002:2013, on es recolliran les No Conformitats (Menors i Majors) així com les Observacions.

6.4.3. Informe de l'auditoria

El treball de camp culmina amb la transferència a l'auditat i al client de l'auditoria (en aquest cas són el mateix pel fet de ser una auditoria interna de primera part) dels resultats obtinguts. S'analitzen les proves fetes i es determina si els resultats es poden catalogar com a proves d'auditoria i si són rellevants per a determinar conclusions alineades amb l'objectiu de l'auditoria. Aquestes conclusions s'exposen en un document final anomenat "Informe d'Auditoria".

6.4.4. Seguiment de l'auditoria

Les conclusions de l'auditoria portaran a l'auditat a realitzar actuacions amb l'objectiu de corregir els defectes que s'han evidenciat. En els casos d'auditories internes de primera part és normal que s'ofereixi una revisió dels punts auditats i es suggereixin propostes de solució ja que aquest punt és un dels objectius de l'auditoria.

Aquestes propostes de solució s'haurien d'incorporar a la revisió del "Pla de Projectes" que ha de servir per a evolucionar el sistema de la "Fase Objectiu", la qual estem auditant, i la "Fase Pilar" que és el resultat final del procés i que portarà a la nostra organització a estar en disposició de realitzar una "Auditoria de Certificació" de la norma.

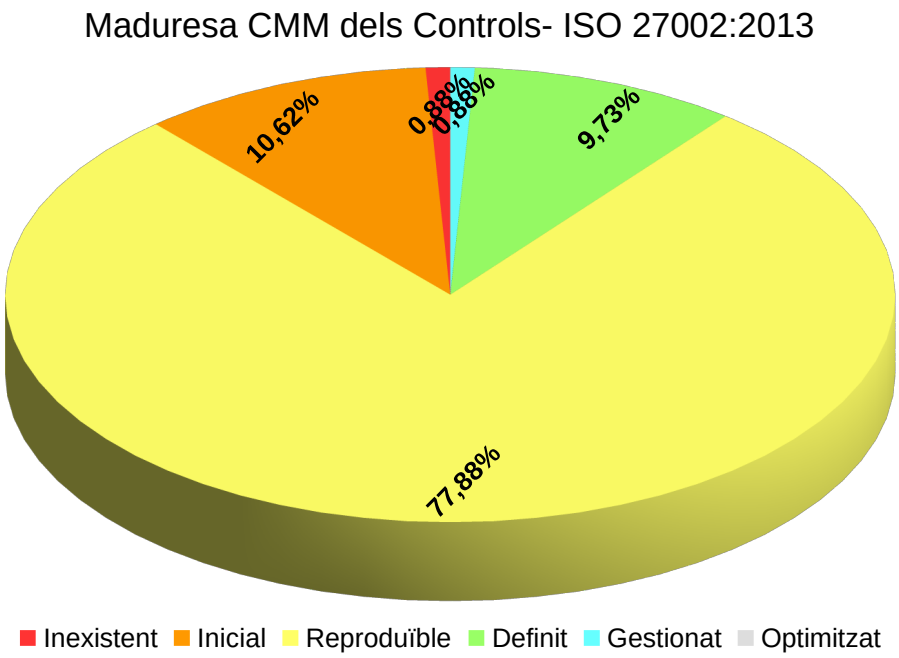
6.5. Resum executiu

Un cop realitzada l'auditoria d'avaluació de l'estat de la maduresa del SGSI de l'Ajuntament de Fita Alta utilitzant com a referència el catàleg de controls de la Norma ISO/IEC 27002:2013 s'han obtingut un conjunt de resultats que permeten avaluar l'estat del Sistema de Gestió de la Seguretat de la Informació de l'Ajuntament de Fita Alta.

El resultat de l'auditoria ha donat:

- 1 No-Conformitats majors
- Múltiples No-Conformitats menors

L'avaluació del nivell de maduresa dels controls obtingut de l' "Anàlisi diferencial" realitzat amb l'eina PILAR després d'una avaluació completa i detallada. Ens mostra la gràfica percentual del nivell de maduresa dels 114 controls i dona una visió de conjunt de l'estat de la seguretat.



Com s'havia planificat a l'inici del projecte d'implantació del SGSI, el resultat de la implantació de tots els projectes ens situa a un nivell intermedi previ a l'assoliment dels nivell exigits per la norma.

Només el 9,73% dels controls tenen el nivell de maduresa "L3-Definit" que seria el que demanaria la norma.

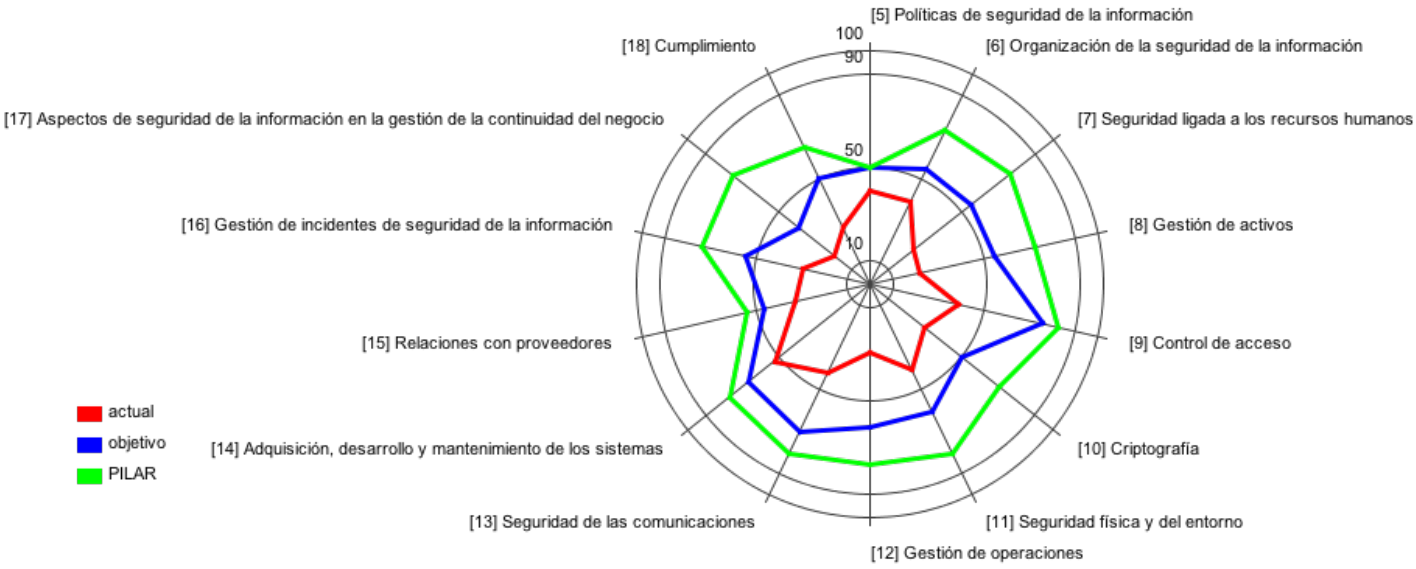
La majoria de controls, el 77,88%, tenen el nivell "L2-Reproduïble" que pot variar entre el 50% i el 90% del compliment de la norma. Aquesta gran quantitat de controls que es troben a l'estat previ del compliment posa de manifest que

cal fer un nou "Pla de projectes" per a implantar les mesures que facin que arribem als nivells de compliment.

Cal veure positivament que el nombre de controls que estan als nivells "L0-Inexistent" i "L1-Inicial" només representen el 11,5% dels controls. Tot i que aquests controls evidencien les mancances més greus i les No-conformitats majors de la norma, el seu reduït nombre permetrà que sigui fàcil que el nou "Pla de Projectes" pugui focalitzar esforços en resoldre-les.

Donat que l'estadi de la implantació del nostre SGSI en el moment de fer l'auditoria ja sabíem que no assoliria els nivells necessaris per a fer una certificació el que volem saber és si el resultat de la implantació del nostre "Pla de Projectes" ha estat satisfactori i ha significat una acostament significatiu als objectius finals del projecte que no són altres que el compliment de la norma.

Aquesta informació la podem veure al gràfic de Radar del compliment. El programa PILAR permet veure el percentatge de mesures de seguretat aplicades a la "fase objectiu" i comparar-les amb els nivells mínims obligatoris definits per la norma i representats a la "fase PILAR".



El gràfic següent ens permet veure quina és la situació de la fase auditada, la fase de color blau anomenada "fase objectiu". L'estat del nostre SGSI a l'inici i abans de la implantació del "Pla de Projectes" és la fase de color vermell anomenada "fase actual". La fase de color verd anomenada "fase PILAR" indica els nivells mínims recomanats per la norma.

El gràfic ens mostra que és una evidència que hi ha hagut un avenç significatiu dels nivells de la fase vermella a la fase blava. Fins i tot s'han assolit els nivell demanats en el domini "5-Polítiques de seguretat". S'ha millorat en tots els dominis, encara que en el domini "17-Gestió de la continuïtat" és on queda més feina per fer.

Anem a veure el detall del compliment de cadascun dels 14 dominis i 35 objectius de control de la norma reflectits per l'auditoria de maduresa. Com que mostrarem només dominis i objectius, si no s'assoleix totalment el nivell de maduresa es marca el nivell dintre del percentatge estimat. En cas que s'assoleixi el nivell de la norma es marcarà de color verd la columna [Norma] per a indicar que s'ha assolit en aquest estadi el nivell exigit.

[L0] Inexistent	0%
[L1] Inicial	1 - 10%
[L2] Repetible però intuitiu	11 - 50%
[L3] Definit	51 - 90%
[L4] Gestionat	91 - 95%
[L5] Optimitzat	96 - 100%

	[Inicial]	[Auditat]	[Norma]
[5] Políticas de seguridad de la información	**L1-L2 40%**	**L2 50%**	**L2 50%**
[5.1] Dirección de la gestión de la seguridad de la información	L1-L2 40%	L2 50%	L2 50%

	[Inicial]	[Auditat]	[Norma]
[6] Organización de la seguridad de la información	**L0-L3 39%**	**L1-L3 L2-54%**	**L2-L3 73%**
[6.1] Organización interna	L0-L3 53%	L2-L3 L2-79%	L2-L3 76%
[6.2] Dispositivos móviles y teletrabajo	L0-L2 25%	L1-L2 L2-30%	L2-L3 70%

	[Inicial]	[Auditat]	[Norma]
[7] Seguridad ligada a los recursos humanos	**L0-L3 23%**	**L1-L3 L3-55%**	**L2-L4 76%**
[7.1] Antes del empleo	L0-L3 21%	L1-L3 L2-45%	L2-L3 80%
[7.2] Durante el empleo	L0-L3 31%	L2-L3 L3-60%	L2-L4 68%
[7.3] Cese del empleo o cambio de puesto de trabajo	L0-L2 17%	L1-L3 L2-60%	L2-L3 80%

	[Inicial]	[Auditat]	[Norma]
[8] Gestión de activos	**L0-L3 22%**	**L1-L3 L3-55%**	**L2-L4 72%**
[8.1] Responsabilidad sobre los activos	L0-L3 28%	L1-L3 L3-62%	L2-L3 73%
[8.2] Clasificación de la información	L0-L2 12%	L1-L3 L2-43%	L2-L3 73%
[8.3] Manipulación de los soportes	L0-L3 24%	L1-L3 L3-59%	L2-L4 70%

	[Inicial]	[Auditat]	[Norma]
[9] Control de acceso	**L0-L3 39%**	**L1-L4 L3-76%**	**L2-L5 83%**
[9.1] Requisitos de negocio para el control de acceso	L0-L3	L2-L3	L2-L3

	26%	L3-65%	68%
[9.2] Gestión del acceso de usuario	L0-L3 39%	L1-L4 L3-75%	L2-L4 84%
[9.3] Responsabilidades de usuario	L2 50%	L4 95%	L4 95%
[9.4] Control de acceso al sistema y a las aplicaciones	L0-L3 39%	L1-L3 L3-67%	L2-L5 83%

	[Inicial]	[Auditat]	[Norma]
[10] Criptografía	**L0-L3 30%**	**L1-L3 L2-50%**	**L2-L5 70%**
[10.1] Controles criptográficos	L0-L3 30%	L1-L3 L2-50%	L2-L5 70%

	[Inicial]	[Auditat]	[Norma]
[11] Seguridad física y del entorno	**L0-L3 41%**	**L0-L3 L3-60%**	**L2-L5 81%**
[11.1] Áreas seguras	L0-L3 46%	L1-L3 L3-62%	L2-L4 84%
[11.2] Equipos	L0-L3 36%	L0-L3 L3-59%	L2-L5 77%

	[Inicial]	[Auditat]	[Norma]
[12] Gestión de operaciones	**L0-L3 29%**	**L0-L3 L3-61%**	**L2-L4 78%**
[12.1] Responsabilidades y procedimientos de operación	L0-L3 35%	L1-L3 L3-51%	L2-L3 72%
[12.2] Protección contra el código malicioso	L0-L3 33%	L2-L3 L3-70%	L2-L4 78%
[12.3] Copias de seguridad	L0-L3 42%	L2-L3 L3-77%	L2-L3 83%
[12.4] Registro y monitorización	L0-L3 33%	L1-L3 L3-61%	L2-L4 76%
[12.5] Control del software en explotación	L0-L3 30%	L1-L3 L3-57%	L2-L4 71%
[12.6] Gestión de las vulnerabilidades técnicas	L0-L3 26%	L0-L3 L3-62%	L2-L4 74%
[12.7] Consideraciones sobre la auditoría de los sistemas de información	L0-L1 5%	L2 50%	L3 90%

	[Inicial]	[Auditat]	[Norma]
[13] Seguridad de las comunicaciones	**L0-L3 42%**	**L1-L3 L3-70%**	**L2-L5 81%**
[13.1] Gestión de la seguridad de las redes	L0-L3 59%	L2-L3 L3-80%	L2-L5 84%
[13.2] Transferencia de información	L0-L3 26%	L1-L3 L3-60%	L2-L3 77%

	[Inicial]	[Auditat]	[Norma]
[14] Adquisición, desarrollo y mantenimiento de los sistemas	**L0-L3 53%**	**L0-L3 L3-67%**	**L2-L4 77%**
[14.1] Requisitos de seguridad de los sistemas de información	L0-L3 35%	L1-L3 L3-59%	L2-L4 67%
[14.2] Seguridad en los procesos de desarrollo y	L0-L3	L0-L3	L2-L3

soporte	34%	L3-52%	75%
[14.3] Datos de prueba	L3 90%	L3 90%	L3 90%

	[Inicial]	[Auditat]	[Norma]
[15] Relaciones con proveedores	**L0-L3 33%**	**L1-L3 L2-47%**	**L2-L3 54%**
[15.1] Seguridad de la información en las relaciones con proveedores	L0-L3 31%	L1-L3 L2-44%	L2-L3 53%
[15.2] Gestión de servicios prestados por terceros	L0-L3 35%	L1-L3 L2-50%	L2-L3 54%

	[Inicial]	[Auditat]	[Norma]
[16] Gestión de incidentes de seguridad de la información	**L0-L3 30%**	**L1-L3 L3-55%**	**L2-L3 74%**
[16.1] Gestión de incidentes de seguridad de la información y mejoras	L0-L3 30%	L1-L3 L3-55%	L2-L3 74%

	[Inicial]	[Auditat]	[Norma]
[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**L0-L3 20%**	**L0-L3 L2-39%**	**L2-L3 75%**
[17.1] Continuidad de la seguridad de la información	L0-L3 3%	L0-L3 L2-25%	L2-L3 76%
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	L0 36%	L0-L1 L3-54%	L3 75%

	[Inicial]	[Auditat]	[Norma]
[18] Cumplimiento	**L0-L3 27%**	**L1-L3 L3-51%**	**L2-L4 65%**
[18.1] Cumplimiento de los requisitos legales y contractuales	L0-L3 34%	L2-L3 L3-56%	L2-L3 62%
[18.2] Revisiones de seguridad de la información	L0-L2 20%	L1-L3 L2-46%	L2-L4 69%

Aquesta informació a nivell de dominis i objectius de control presenta un percentatge de nivells L3 superior al de nivells L2 que no és correspon als valors individuals dels controls mostrat al gràfic del nivell de maduresa. El gràfic és el que mostra el valor real auditat mentre que les taules prèvies es mostren a nivell orientatiu del nivell dels 14 dominis de la norma ISO/IEC 27002:2013.

6.6. Recomanacions

L'estudi dels resultats de l'auditoria de l'avaluació de la maduresa dels controls de la norma ISO/IEC 27002:2013 aconsella realitzar les següents actuacions:

1.- Prendre mesures per a corregir les No-conformitats majors de forma urgent
En aquest cas això implica el desenvolupament del Pla de Continuïtat i la seva implantació a l'Ajuntament de Fita Alta.

2.- Realització d'un nou Pla de projectes
Realització d'un nou Pla de projectes amb un termini de 12 mesos per a la seva realització que porti el nostre sistema a l'estat de maduresa actual a una nova fase que assoleixi el compliment de la norma.

El nou Pla de Projectes s'ha de basar en la solució de les No-conformitats (majors i menors) detectades a l'auditoria de compliment i en l'aplicació de les mesures correctores resultants de l'actualització de l'anàlisi de riscos.

3.- Planificació d'una nova auditoria de maduresa dels controls de la norma
Un cop finalitzada l'execució del nou Pla de projectes car tornar a fer una auditoria de maduresa per a avaluar l'estat del sistema i l'efectivitat del Pla de Projectes.

4. Fer una auditoria de certificació de la norma ISO/IEC 27001:2013
Si el resultat de l'auditoria de maduresa anterior és satisfactori cal plantejar-se la certificació del sistema. S'aconsella planificar la realització de l'auditoria de certificació en un termini de 6 mesos després de la realització de l'auditoria de maduresa.

6.7. Detall de l'informe – llista detallada de les constatacions

Una **No-conformitat** és l'absència o fallada en la implantació o el manteniment d'un element o més requerits pel sistema de gestió, o bé una situació que, basant-se en evidències objectives, pot comportar un dubte raonable sobre la capacitat de l'SGSI de cobrir els objectius de seguretat de la companyia o del compliment de la política de seguretat.

Una no-conformitat pot ser relativa a la política de seguretat, a l'estàndard de gestió de seguretat de la informació, a procediments o a requisits legals. S'identifiquen tres tipus de no-conformitats, segons la criticitat de l'incompliment: "**no-conformitat major**", "**no-conformitat menor**" i "**observacions**".

Generalment es considera no-conformitat major l'absència de qualsevol dels controls essencials que determina l'ISO 27002. Alguns exemples de no-conformitat major són absència de l'anàlisi de riscos, absència d'un sistema de gestió d'incidències, absència d'un pla de continuïtat de negoci, absència de procediments per a gestionar registres, canvis en l'SGSI sense aprovació formal, incompliment reiterat d'un procediment, i un nombre elevat de no-conformitats sobre una mateixa secció de la norma o un mateix departament.

Val a dir que en aquest moment farem el criteri de valoració de No-conformitats tot i no estar realitzant una auditoria de certificació sinó una d'avaluació de la maduresa de la norma. Aquesta valoració permetrà que les "No-Conformitats majores" detectades siguin els principals objectius de millora del nou Pla de Projectes que s'ha de realitzar.

Les valoracions del compliment de la norma i els intervals utilitzats per a la identificació de No-conformitats estan extrets de l'informe "Cumplimiento de la Norma ISO/IEC 27002:2013" extret de l'eina PILAR. Aquest informe mostra de forma gràfica i quantitativa el compliment de la norma en les modalitats de nivell de maduresa i en percentatge.

En les gràfiques mostrades a l'informe i dels quals es mostren algunes parts en aquest informe d'auditoria, els codis de colors corresponen a :

- [actual] situació a l'inici del projecte
- [objetivo] situació objectiu. Situació actual en el moment de l'auditoria
- [PILAR] recomanació de la norma ISO/IEC 27001:2013

6.7.1. No-Conformitats majors

És la relació de les "No-Conformitats majors", o "No-conformitats molt greus" que impedirien la certificació en cas que aquest fos l'objectiu de l'auditoria. L'existència de múltiples No-Conformitats majors en casos d'auditoria de certificació pot arribar a fer que s'aturi el procés d'auditoria.

Donat que no s'ha realitzat una auditoria real per a la realització d'aquest apartat s'ha utilitzat un criteri alternatiu que serveixi per a mostrar les no conformitats.

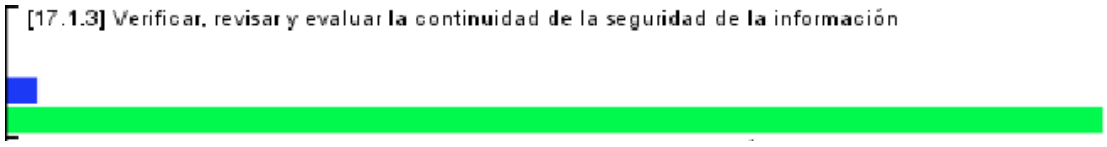
Considerarem que estem davant d'una "No-Conformitat major", basant-nos en el nivell de maduresa, quan els nivells assolits pel control en el compliment de la norma tenen un interval de compliment dels nivells de la "fase objectiu" per sota de l'interval dels nivells de la "Fase PILAR" que és la que marcaria la norma. Seguint aquest criteri s'ha detectat 1 No-conformitats majors.

S'han detectat una No-Conformitats majors

NC01

Id. No-Conformitat	**NC01**
Tipus de no conformitat	**Major** / ~~Menor~~
Descripció	Inexistència del Pla de Continuïtat de l'organització, la qual cosa fa que la seva verificació, revisió i avaluació no siguin possibles.
Paràgrafs de la norma afectats	17.1.3 Verificar, revisar i avaluar la continuïtat de la seguretat de la informació.
Acció correctora	Elaboració del Pla de Continuïtat de Negoci de l'organització.

En el domini "17. Aspectes de la seguretat de la informació en la gestió de la continuïtat del negoci" en l'objectiu "17.1. Continuïtat de la seguretat de la informació" en el control "17.1.3 Unificar, revisar i avaluar la continuïtat de la seguretat de la informació".



Maduresa	[actual]	[objetivo]	[PILAR]
[17.1] Continuidad de la seguridad de la información	L0-L3	L0-L3	L2-L3
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	L0	L0-L1	L3

[17.1] Continuidad de la seguridad de la información	3%	25%	76%
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	0%	3%	90%

6.7.2. No-Conformitats menors

A continuació es mostra una relació d'algunes de les No-Conformitats menors, que per la seva naturalesa no arriben a la gravetat de les anteriors.

Considerarem que estem davant d'una "No-Conformitat menor" quan els nivells assolits pel control en el compliment de la norma tenen dintre del seu l'interval de compliment dels nivells de la "fase objectiu" el nivell que li correspondria a la "Fase PILAR" que és la que marcaria la norma. Seguint aquest criteri s'ha detectat múltiples No-conformitats menors que no es reporten en la seva totalitat.

Gairebé tots els 35 objectius de control dels 14 dominis tenen No-conformitats menors. Això és així ja que l'auditoria de compliment es realitza només un any després de l'inici de la implantació del SGSI el qual requeria un període de 2 anys per a la implantació en la seva totalitat.

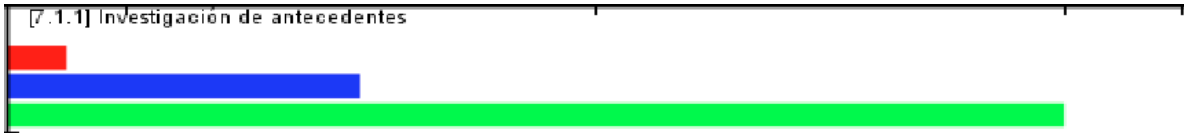
Mostrarem, com a exemple, 3 de les No-Conformitats menors associades als controls :

- 7.1.1 Investigació dels antecedents
- 13.2.1 Polítiques i procediments de transferència d'informació
- 16.1.7 Recopilació d'evidències

NC02

Id. No-Conformitat	**NC02**
Tipus de no conformitat	~~Major~~ / **Menor**
Descripció	Es realitza una insuficient comprovació, prèvia a la contractació, dels antecedents dels treballadors que es dediquen a la gestió de la seguretat del sistema d'informació.
Paràgrafs de la norma afectats	7.1.1 Investigació d'antecedents
Acció correctora	Informar-se dels antecedents dels treballadors abans de formalitzar la contractació.

Constatació en el domini "7. Seguretat lligada als recursos humans" en l'objectiu "7.1. Abans de la contractació" en el control "7.1.1 Investigació dels antecedents"



Maduresa	[actual]	[objetivo]	[PILAR]
[7.1] Antes del empleo	L0-L3	L1-L3	L2-L3
[7.1.1] Investigación de antecedentes	L0-L1	L1-L2	L3

[7.1] Antes del empleo	21%	45%	80%
[7.1.1] Investigación de antecedentes	5%	30%	90%

NC03

Id. No-Conformitat	**NC03**
Tipus de no conformitat	~~Major~~ / **Menor**
Descripció	Inexistència de Polítiques i procediments que regulin la transferència d'informació..
Paràgrafs de la norma afectats	13.2.1 Polítiques i procediments de transferència d'informació
Acció correctora	Elaborar la Política de Transferència d'Informació i desenvolupar els seus procediments.

Domini 13. Seguretat en les telecomunicacions, objectiu 13.2. Abans de la contractació" control 13.2.1 Polítiques i procediments de transferència d'informació

Maduresa	[actual]	[objetivo]	[PILAR]
[13.2] Transferencia de información	L0-L3	L1-L3	L2-L3
[13.2.1] Políticas y procedimientos de transferencia de información	L0-L1	L1-L2	L3
[13.2] Transferencia de información	26%	60%	77%
[13.2.1] Políticas y procedimientos de transferencia de información	5%	40%	90%

NC04

Id. No-Conformitat	**NC04**
Tipus de no conformitat	Major / **Menor**
Descripció	No es recullen les evidències dels incidents de seguretat seguint un procediment que permeti la seva utilització en un procés de peritatge amb un caràcter provatori o de dictamen.
Paràgrafs de la norma afectats	16.1.7 Gestió d'incidents de seguretat de la informació i millores
Acció correctora	Elaborar el procediments de recollida d'evidències i fer formació al personal de TI que l'haurà d'aplicar.

En el domini "16. Gestió d'incidents de seguretat de la informació" en l'objectiu "16.1. Gestió d'incidents de seguretat de la informació i millores" en el control "16.1.7 Recopilació d'evidències".

Maduresa	[actual]	[objetivo]	[PILAR]
[16.1] Gestión de incidentes de seguridad de la información y mejoras	L0-L3	L1-L3	L2-L3
[16.1.7] Recopilación de evidencias	L0-L1	L1-L2	L3
[16.1] Gestión de incidentes de seguridad de la información y mejoras	30%	55%	74%
[16.1.7] Recopilación de evidencias	5%	30%	90%

6.7.3. Observacions

Les observacions són comentaris sobre característiques concretes dels controls quan aquests estan a un nivell superior al que demana la norma.

En posarem un a tall d'exemple.

Id. Observació	OBS01
Descripció	La Política de Seguretat de contempla el procediment de revisió de la política de seguretat. Des que es va aprovar per decret d'alcaldia hi ha hagut una revisió per a adaptar-la a canvis organitzatius en l'equip municipal.
Paràgrafs de la norma afectats	5.1.2 Revisió de les polítiques de seguretat de la informació

6.8. Conclusions de l'auditoria

Els nivells de seguretat que l'eina PILAR recomana per a la implantació de la norma es mostren en la fase anomenada "PILAR". La transició entre la "fase objectiu" i la "fase PILAR" hauria de ser motiu una nova anàlisi de riscos realitzada a la fi de la "fase objectiu" i que permetés elaborar noves accions incloses en una revisió del Pla de Millora que hauria de durar aproximadament el mateix que per a la fase anterior, entre 6 mesos i 1 any. Així en un període de 2 anys assoliríem en ple compliment de la norma.

7. Conclusions

El Pla Director de la Seguretat de la Informació servirà per a que l'Ajuntament de Fita Alta tingui una fulla de ruta que li permeti gestionar d'una forma sistemàtica i adequada la seguretat dels seus sistemes d'informació.

La millor manera de gestionar la seguretat és utilitzar uns estàndards reconeguts internacionalment que garanteixin que es fa un ús correcte dels sistemes d'informació que ajudi a millorar la confiança que els ciutadans tenen en l'administració electrònica.

La realització del Pla Director ha significat treballar la capacitació i els coneixements necessaris per a la implantació d'un SGSI. El mateix procés seguit durant la implantació és similar al que la norma ISO/IEC 27001 proposa per al seu manteniment i millora al llarg del temps. És el que anomenem cicle de Deming o de millora contínua PDCA (**P**lan, **D**o, **C**heck, **A**ct).

Un cop implantat el nostre SGSI haurem fet un cilce sencer i tornarem a estar a la primera fase, la fase **P**lan (de **P**lanificació) on revisarem l'adequació de la Política de seguretat, l'abast del SGSI, les polítiques d'alt nivell i els objectius de seguretat. Un cop revisats aquests punts tornarem a realitzar una anàlisi de riscos i actualitzarem l'avaluació de l'impacte residual que la nostra organització està disposada a assumir. Totes aquestes habilitats i competències les hem treballat a la fase 1 (*Objectius i anàlisi diferencial*), la fase 2 (*Sistema de Gestió documental*) i la fase 3 (*Anàlisi de riscos*) del TFM.

Un cop realitzada la planificació, es passa a la fase **D**o (**F**er) on implantarem un Pla de Gestió del risc com conjunt de projectes agrupats en un Pla de millora de la seguretat. Aquest Pla contemplarà la selecció i implantació d'indicadors que ens permetran gestionar el procés. Aquestes habilitats i competències s'han treballat a la fase 4 del TFM (*Proposta de projectes*).

Implantades les accions del Pla de Millora només cal monitoritzar el procés de la seguretat i revisar-lo de forma regular utilitzant els indicadors definits. Això és el que es fa a la fase **C**heck (Verificar). També es realitzen auditories internes de forma planificada per a fer una validació més exhaustiva del sistema. Les habilitats necessàries per a la realització de les auditories s'han treballat a la fase 5 del TFM (*Auditoria de compliment*).

El tancament del cicle de millora contínua es produeix a la fase **A**ct (Actuar) que és on s'implanten les millores i les accions correctives i preventives que s'han posat de manifest a l'Auditoria interna del SGSI. Aquesta fase no s'ha treballat de forma explícita en el TFM atès que és una part pròpiament centrada en el manteniment del sistema i és complicat treballar-la de forma efectiva en el disseny d'un Pla Director si el SGSI no està implantat i en funcionament.

Analitzada la feina feta durant el TFM hem de valorar si s'han assolit els objectius definits a l'inici del projecte i en cas que no hagi estat així identificar quins han estat els motius que no ho han permès.

Recordem quins eren els objectius del TFM:

- Compliment de la normativa legal en matèria de seguretat: ENS, LOPD
- Implantació de les bones pràctiques en Seguretat dels SGSI definides a les normes ISO/IEC 27000 (27001:2013 com a norma certificable i 27002:2013 com a recull de bones pràctiques)
- Millorar la seguretat dels sistemes de gestió de la informació de l'Ajuntament
- Oferir serveis segurs a la ciutadania
- Millorar la confiança que tenen els ciutadans en l'administració

L'anàlisi de compliment realitzat a la fase 5 (*auditoria de compliment*) a la meitat del procés d'implantació evidencia una millora significativa del SGSI en el compliment de la norma ISO/IEC 27002:2013 així com la possibilitat d'assolir el compliment efectiu en un any vista, tal i com s'havia planificat inicialment. L'alineació en matèria de seguretat entre les normes ISO/IEC i l'ENS fa que la implantació i compliment d'una d'elles millori significativament la implantació i el compliment de l'altra norma.

En aquest sentit podem afirmar que l'avaluació del procés a la meitat de la seva execució és positiva i els dos primers objectius s'estan assolint. Si el procés marcat pel Pla Director segueix el mateix ritme els objectius s'hauran assolit plenament a la finalització del Pla en el termini previst.

Així mateix, en aquests moments ja podem donar per assolit plenament l'objectiu que el SGSI de l'Ajuntament de Fita Alta ha millorat la seva seguretat. L'aplicació del Pla Director, la implantació de la norma ISO/IEC 27001:2013 i els resultats de l'auditoria de compliment així ho corroboren.

S'han assolit la resta d'objectius? Els serveis que s'ofereixen a la ciutadania són segurs? S'ha millorat la confiança que els ciutadans tenen en l'Administració?. Aquests objectius són de difícil mesura ja que impliquen valoracions subjectives.

Sense cap mena de dubte si millorem la seguretat dels nostres sistemes llavors també haurem fet més segur el servei que s'ofereix al ciutadà. Una altra cosa molt diferent és que la ciutadania sigui capaç de percebre aquest canvi. En matèria de seguretat costa molt generar confiança mentre que la materialització dels incidents sempre generarà una sensació d'inseguretat. No hi ha cap recepta que ens porti a l'assoliment de la confiança que no sigui la utilització de les millors pràctiques que els mercat, la legalitat i les normes ens puguin oferir.

Cal analitzar el seguiment de la planificació i la metodologia utilitzada per a la realització del "Pla Director de Seguretat" per a fer-ne una valoració.

En aquest sentit i amb caràcter general, s''ha seguit la metodologia i la planificació del TFM que es van marcar a l'inici del projecte. Val a dir que s'ha fet una variació important en la metodologia. S'ha utilitzat l'eina EAR-PILAR desenvolupada pel CCN-CERT per a fer l'anàlisi de riscos que segueix la metodologia MAGERIT proposada pel Consell Superior d'Administració

Electrònica. Si bé la metodologia proposada pel TFM és la mateixa, la metodologia MAGERIT, el resultat i la forma de fer l'anàlisi de riscos utilitzant les eines PILAR ha estat molt diferent de la proposada per les guies del TFM.

Hi ha tres versions de l'eina PILAR per a fer l'anàlisi de riscos: EAR-PILAR, PILAR-Bàsic i µPILAR. Es va optar per la utilització de l'eina µPILAR a la fase 3 (*Anàlisi de riscos*) ja que suposadament permetia fer de forma ràpida l'anàlisi de riscos amb una definició bàsica dels actius.

Això no va ser així. És cert que es va partir d'una definició ràpida dels actius essencials i una enumeració de la resta dels actius segons les seves funcions. En canvi la feina d'avaluació de les salvaguardes que permetia calcular el risc real, residual i de les fases definides al projecte ha estat llarga i feixuga. La documentació de µPILAR parlava de fer-ho en "*hores*" i aquesta tasca ha portat "*dies*" de feina, gairebé una setmana.

La qual cosa ha fet que la tria de µPILAR com a eina d'anàlisi de riscos no hagi estat una bona elecció. L'eina EAR-PILAR genera molts més informes que l'eina µPILAR i la seva utilització no aportava un increment significatiu de feina. La tria de l'eina µPILAR, que ara considerem equivocada, ja no va tenir marxa enrere quan es van poder apreciar les mancances que tenia ja que la planificació del TFM estava molt avançada i no permetia fer una nova anàlisi de riscos. Tot i aquest fet, s'ha migrat el projecte de l'eina µPILAR a l'eina EAR-PILAR (perdent un parell de dies de feina en adaptacions i revisions) que ha permès que les fases finals del TFM i els informes utilitzats al lliurament final s'hagin generat amb aquesta versió de l'eina.

L'eina EAR_PILAR, la més completa de les eines desenvolupades pel CCN-CERT, permet una anàlisi exhaustiva dels actius totalment compatible a la descrita per la metodologia i no és limita als actius essencials (d'informació o serveis), punts d'interconnexió de xarxa i contractes de terceres parts com fa l'eina µPILAR. També permet fer una anàlisi quantitativa que µPILAR no permet i que no s'ha realitzat en el desenvolupament d'aquest Pla Director.

Analitzarem les tasques que s'han de treballar en el futur i que no han estat explorades amb prou detall en aquest "Pla Directors de la Seguretat".

Es detecta una millora associada a les tasques i habilitats relacionades amb la fase **A**ct (Actuar) del cicle PDCA que recomana la norma ISO/IEC 27001:2013. Per a treballar les capacitacions necessàries caldria una nova fase després de la realització de l'auditoria que comportés l'aplicació de les millores proposades i això queda fora de lloc en un Pla Director. Aquesta fet implica que aquestes habilitats i tasques s'hauran d'assolir fora del marc del TFM.

L'obligació del compliment dels terminis en la redacció del "Pla Directors de seguretat" ha fet que la definició d'alguns inventaris sigui millorable i s'hagi d'anar perfeccionant en les successives iteracions del nostre cicle de millora contínua de la gestió de la seguretat dels sistemes d'informació. Entre aquests inventaris en podríem destacar el detall dels indicadors implantats en l'SGSI i l'inventari d'actius.

Per finalitzar, farem un recull de les principals conclusions extretes de la realització d'aquest Treball de Final de Màster i de l'elaboració del "Pla Director de Seguretat".

La primera conclusió és que s'han assolit de forma satisfactòria els objectius plantejats a l'inici del projectes.

La segona conclusió és que l'elaboració del Pla Director, a banda d'oferir una fulla de ruta per a la millora de la seguretat a l'Ajuntament de Fita Alta, també ha servit per a adquirir la capacitació i els coneixements necessaris per a la gestió, manteniment i millora al llarg del temps d'un SGSI basat en la norma ISO/IEC 27001:2013.

La tercera conclusió és que l'auditoria de compliment posa de manifest que el SGSI de l'Ajuntament de Fita Alta ha millorat considerablement des de d'inici de l'aplicació del Pla Director. És de preveure que en una nova iteració del cicle PDCA d'una durada de 12 mesos s'assoleixin els nivells de compliment de la norma ISO/IEC 27001:2013 i de la normativa legal en matèria de seguretat: ENS i LOPD.

La quarta conclusió fa referència a la utilització de les eines de gestió de riscos PILAR del CCN-CERT. Si és possible, és recomanable fer-les servir ja que aporten molts més beneficis que inconvenients per al manteniment del sistema al llarg del temps. Això si, és recomana fer servir l'eina complerta, EAR-PILAR, ja que permet una aplicació total de la metodologia MAGERIT.

La última conclusió que ha posat en evidència la realització d'aquest treball és que la gestió de la seguretat dels sistemes d'informació és un procés i no una tasca. No és la implantació d'un producte o servei, és la implantació d'un procediment de gestió que s'ha d'anar monitoritzant de forma permanent, avaluant els seus resultats per a detectar possibles problemes i corregir-los i on s'han de revisar sempre els objectius, l'abast, les polítiques i criteris aplicats per a millorar-los i adequar-los a la realitat de la nostra organització. Així per a la resta dels anys, en un procés sense fi que el que pretén és anar perfeccionant-se a ell mateix de forma progressiva.

Bibliografia

[**PILAR01**] Informació sobre l'eina EAR/PILAR, un entorn per a l'anàlisi de riscos http://www.ar-tools.com/es/index.html

[**MAGERIT01**] Informació sobre la metodologia MAGERIT, Metodologia d'Anàlisis i Gestió de Riscos
http://www.ar-tools.com/magerit/index.html

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[**MAGERIT02**] MAGERIT Libro I: Método, Portal d'administració electrònica
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_método_es_NIPO_630-12-171-8.pdf

[**MAGERIT03**] MAGERIT Libro II: Catálogo de elementos, Portal d'administració electrònica
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_catálogo%20de%20elementos_es_NIPO_630-12-171-8.pdf

[**MAGERIT04**] MAGERIT Libro III: Guía de técnicas, Portal d'administració electrònica
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8/2012_Magerit_v3_libro3_gu%C3%ADa%20de%20técnicas_es_NIPO_630-12-171-8.pdf

[**ENS01**] Esquema Nacional de Seguretat, Portal d'administració electrònica
http://administracionelectronica.gob.es/ctt/ens

[**ENS02**] Esquema Nacional de Seguretat – Certificaciones 27001, Guía de seguridad (CCN-STIC 825), Portal del CCN-CERT
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

[**UOC01**] Apunts de l'assignatura "Sistemes de Gestió de la Seguretat de la Informació", *MISTIC*.

[**UOC02**] Apunts de l'assignatura "Auditoria Tècnica i de Certificació", *MISTIC*

Annex I – Model de maduresa de la capacitat

Model de Maduresa de la Capacitat (CMM):

Efectivitat	CMM	Significat	Descripció
0%	L0	Inexistent	No hi ha una definició de responsabilitats en matèria de seguretat de la informació.
10%	L1	Inicial / Ad-hoc	Les responsabilitats principals s'assignen o assumeixen informalment. Cada persona sap la seva responsabilitat, però no la dels altres.
50%	L2	Repetible, però intuïtiu	Se sap qui assumeix les funcions principals en matèria de seguretat de les TIC i de la resta del negoci, però les funcions de seguretat no estan definides ni documentades específicament, sinó que s'assumeixen individualment com a part d'altres funcions (per exemple, la direcció d'un projecte).
90%	L3	Definit	Existeix, amb algunes deficiències. Les responsabilitats en seguretat de la informació s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, s'han donat a conèixer i s'ha fet o planificat la capacitació de totes les persones que ho requereixin.
95%	L4	Gestionat i mesurable	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, però no es fa una revisió anual per a verificar que totes les funcions s'han assignat bé i que els responsables desenvolupen la seva funció.
100%	L5	Optimitzat	Les responsabilitats s'han definit i documentat en tots els nivells del negoci, les ha aprovades i assignades la direcció, se n'ha fet difusió entre el personal i formació a aquells que requerien coneixements específics, es revisa periòdicament el desenvolupament d'aquestes funcions i hi ha un procés per a detectar deficiències en l'assignació i coordinació de funcions i per a aplicar-hi correccions.

Annex II – Plantilla d'Indicadors

Plantilla que farem servir per a la definició dels indicadors.

Nom d'indicadors	
Descripció	
Control de seguretat	
Fórmula de mesurament	
Unitats de mesura	
Freqüència de mesurament	
Valor objectiu **Valor llindar**	
Responsable de la mesura	

Annex III – Fitxes de No-Conformitats

Model de fitxa per a recollir la informació de les No-Conformitats

Id. No-Conformitat	
Tipus de no conformitat	Major / Menor
Descripció	
Paràgrafs de la norma afectats	
Acció correctora	

Model de fitxa per a recollir la informació de les observacions

Id. Observació	
Descripció	
Paràgrafs de la norma afectats	

Plantilla que farem servir per a la definició de les fases del projecte

Annex IV – Compliment de la Norma 27002:2013 PILAR (Nivells de Maduresa i percentatge de compliment)

Informe extret de l'eina PILAR.

Cumplimiento Norma ISO/IEC 27002:2013

[2700AJFITA] 2700-Aj_FitaAlta

27.4.2016

1 Introducción

Código: 2700AJFITA
Nombre: 2700-Aj_FitaAlta

Descripción:

Anàlisi de riscos seguint la metodologia MAGERIT utilitzant l'aplicació micro Pilar per al treball de fi de Màster de la UOC amb l'organització fictícia "Ajuntament de Fita Alta"

Datos administrativos:

- desc: Anàlisi de Riscos de l'Ajuntament de Fita Alta -
- resp: Andreu Retamero Pallarès
- org: Ajuntament de Fita Alta
- ver: 1.0
- date: 12/04/2016

Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

2 Valoració del sistema

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

essential

activo	[D]	[I]	[C]	[A]	[T]
[LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]
[INFOPUB] Informació pública	[1](1)	[4](2)	[0](3)	[4]	[0]
[CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
[VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4](4)
[TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
[NOT-ELEC] Notificacions telemàtiques	[1](5)	[4]	[4]	[4]	[4]
[IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
[CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
[POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]

(1) Informació publica: calendari contribuent, ordenances, extractes dels acords de la JG, reglaments.. La no disponibilitat d'aquesta informació no suposa cap interrupció de servei, ni afecta a la productivitat i es pot obtenir per un altre canal (presencial o telefònic)

(2) La manipulació de la informació pública no causaria pèrdues econòmiques però si danys en la imatge de l'ajuntament davant tercers.
[b] por afectar gravemente a las relaciones con el público en general

(3) La informació és pública

(4) [cei] Intereses Comerciales / Económicos:

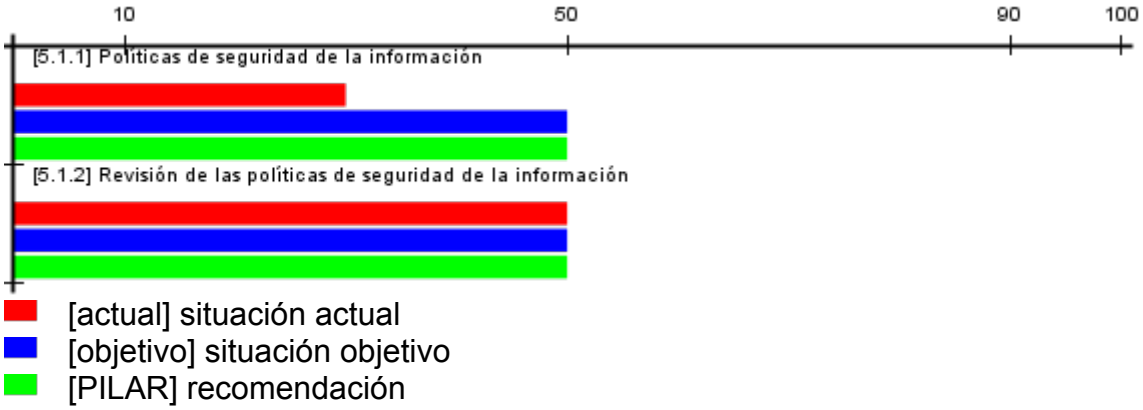
(5) [1.da] Pudiera causar la interrupción de actividades propias de la Organización

3 Controls

Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

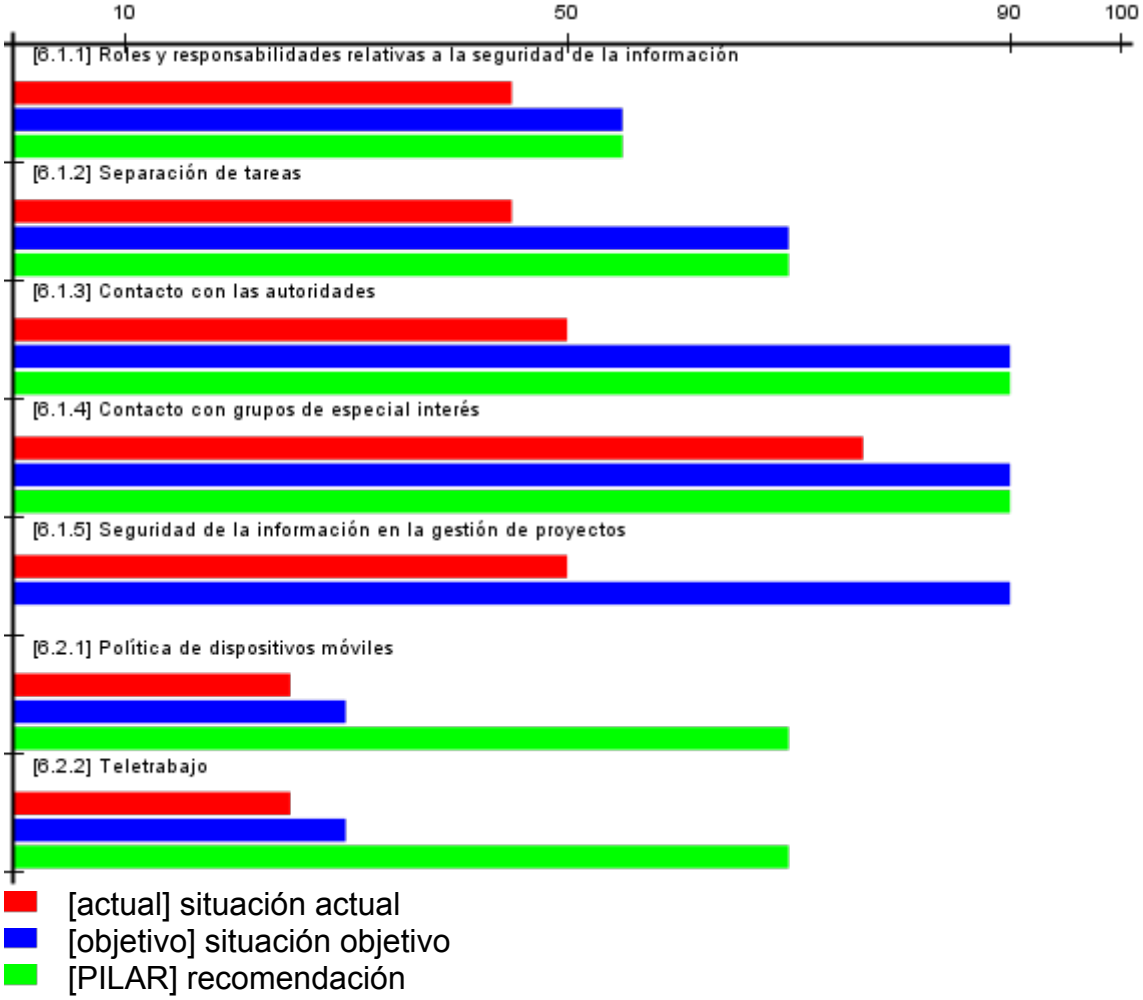
[5] Políticas de seguridad de la información



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[5] Políticas de seguridad de la información	L1-L2	L2	L2
[5.1] Dirección de la gestión de la seguridad de la información	L1-L2	L2	L2
[5.1.1] Políticas de seguridad de la información	L1-L2	L2	L2
[5.1.2] Revisión de las políticas de seguridad de la información	L2	L2	L2

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[5] Políticas de seguridad de la información	40%	50%	50%
[5.1] Dirección de la gestión de la seguridad de la información	40%	50%	50%
[5.1.1] Políticas de seguridad de la información	30%	50%	50%
[5.1.2] Revisión de las políticas de seguridad de la información	50%	50%	50%

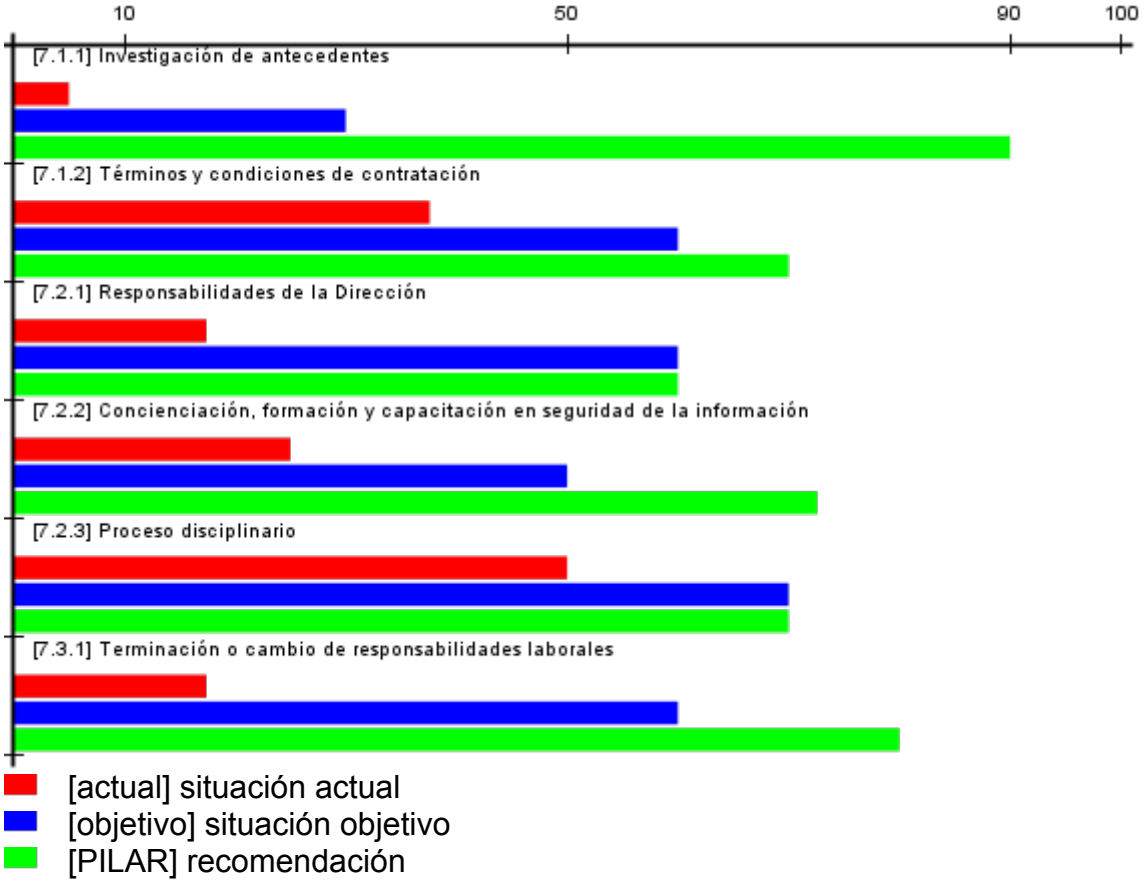
[6] Organización de la seguridad de la información



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[6] Organización de la seguridad de la información	L0-L3	L1-L3	L2-L3
[6.1] Organización interna	L0-L3	L2-L3	L2-L3
[6.1.1] Roles y responsabilidades relativas a la seguridad de la información	L1-L3	L2-L3	L2-L3
[6.1.2] Separación de tareas	L0-L3	L2-L3	L2-L3
[6.1.3] Contacto con las autoridades	L2	L3	L3
[6.1.4] Contacto con grupos de especial interés	L2-L3	L3	L3
[6.1.5] Seguridad de la información en la gestión de proyectos	L2	L3	n.a.
[6.2] Dispositivos móviles y teletrabajo	L0-L2	L1-L2	L2-L3
[6.2.1] Política de dispositivos móviles	L0-L2	L1-L2	L2-L3
[6.2.2] Teletrabajo	L0-L2	L1-L2	L2-L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[6] Organización de la seguridad de la información	39%	54%	73%
[6.1] Organización interna	53%	79%	76%
[6.1.1] Roles y responsabilidades relativas a la seguridad de la información	45%	55%	55%
[6.1.2] Separación de tareas	45%	70%	70%
[6.1.3] Contacto con las autoridades	50%	90%	90%
[6.1.4] Contacto con grupos de especial interés	77%	90%	90%
[6.1.5] Seguridad de la información en la gestión de proyectos	L2	L3	n.a.
[6.2] Dispositivos móviles y teletrabajo	25%	30%	70%
[6.2.1] Política de dispositivos móviles	25%	30%	70%
[6.2.2] Teletrabajo	25%	30%	70%

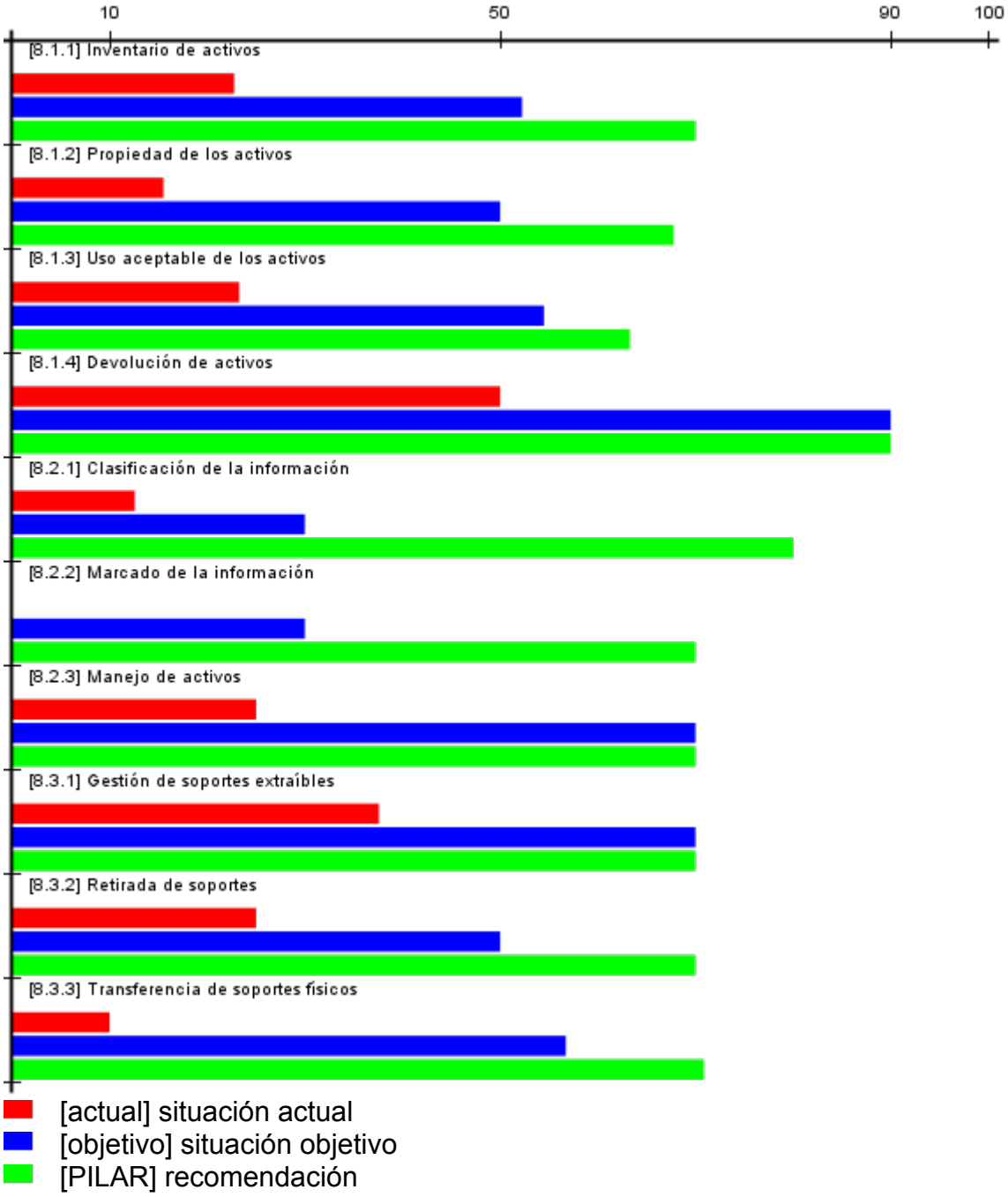
[7] Seguridad ligada a los recursos humanos



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[7] Seguridad ligada a los recursos humanos	L0-L3	L1-L3	L2-L4
[7.1] Antes del empleo	L0-L3	L1-L3	L2-L3
[7.1.1] Investigación de antecedentes	L0-L1	L1-L2	L3
[7.1.2] Términos y condiciones de contratación	L0-L3	L1-L3	L2-L3
[7.2] Durante el empleo	L0-L3	L2-L3	L2-L4
[7.2.1] Responsabilidades de la Dirección	L0-L2	L2-L3	L2-L3
[7.2.2] Concienciación, formación y capacitación en seguridad de la información	L0-L2	L2	L2-L4
[7.2.3] Proceso disciplinario	L1-L3	L2-L3	L2-L3
[7.3] Cese del empleo o cambio de puesto de trabajo	L0-L2	L1-L3	L2-L3
[7.3.1] Terminación o cambio de responsabilidades laborales	L0-L2	L1-L3	L2-L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[7] Seguridad ligada a los recursos humanos	23%	55%	76%
[7.1] Antes del empleo	21%	45%	80%
[7.1.1] Investigación de antecedentes	5%	30%	90%
[7.1.2] Términos y condiciones de contratación	38%	60%	70%
[7.2] Durante el empleo	31%	60%	68%
[7.2.1] Responsabilidades de la Dirección	17%	60%	60%
[7.2.2] Concienciación, formación y capacitación en seguridad de la información	25%	50%	73%
[7.2.3] Proceso disciplinario	50%	70%	70%
[7.3] Cese del empleo o cambio de puesto de trabajo	17%	60%	80%
[7.3.1] Terminación o cambio de responsabilidades laborales	17%	60%	80%

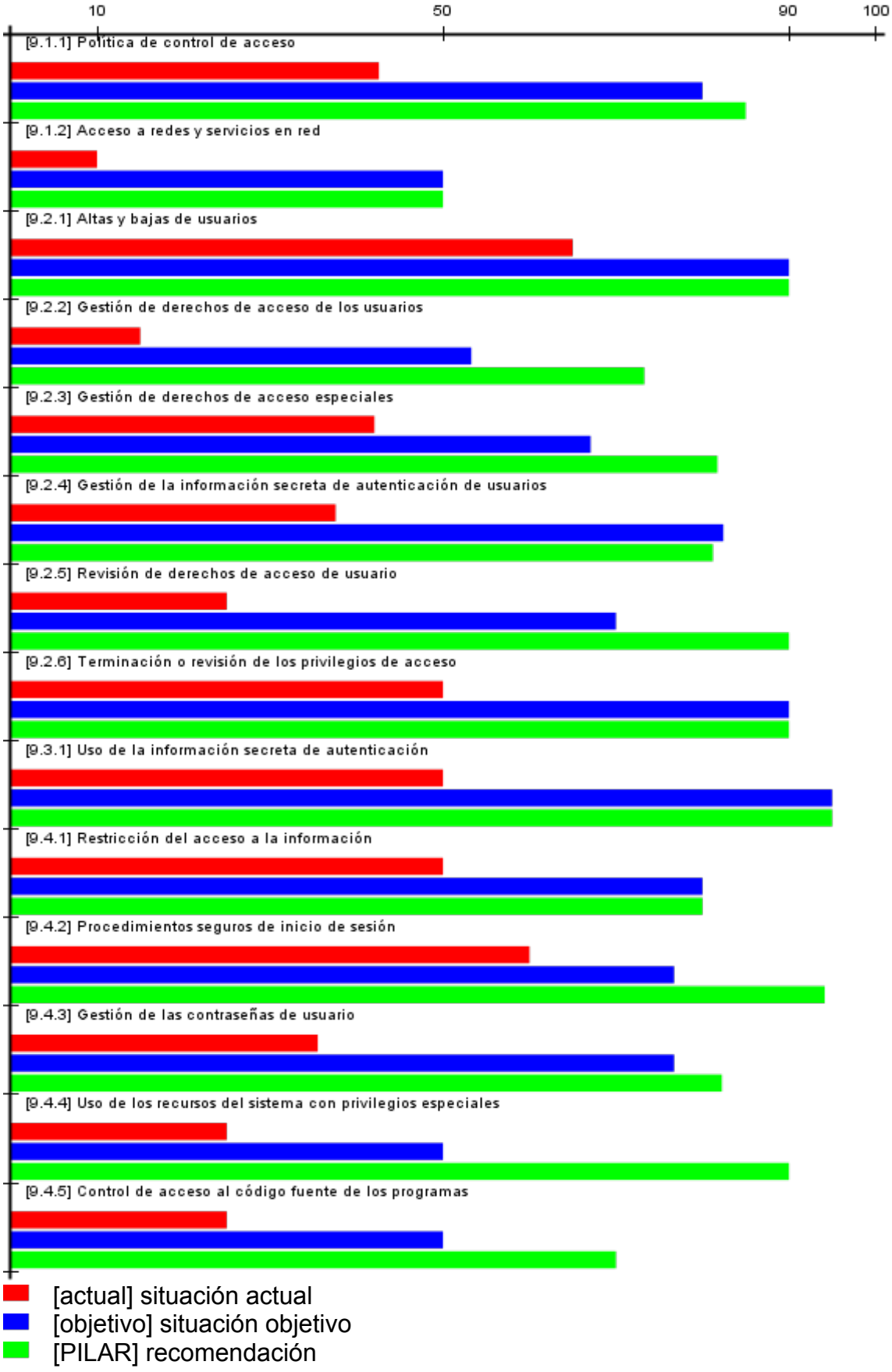
[8] Gestión de activos



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[8] Gestión de activos	L0-L3	L1-L3	L2-L4
[8.1] Responsabilidad sobre los activos	L0-L3	L1-L3	L2-L3
[8.1.1] Inventario de activos	L0-L3	L1-L3	L2-L3
[8.1.2] Propiedad de los activos	L0-L2	L1-L3	L2-L3
[8.1.3] Uso aceptable de los activos	L0-L3	L1-L3	L2-L3
[8.1.4] Devolución de activos	L2	L3	L3
[8.2] Clasificación de la información	L0-L2	L1-L3	L2-L3
[8.2.1] Clasificación de la información	L0-L2	L1-L2	L2-L3
[8.2.2] Marcado de la información	L0	L1-L2	L2-L3
[8.2.3] Manejo de activos	L0-L2	L2-L3	L2-L3
[8.3] Manipulación de los soportes	L0-L3	L1-L3	L2-L4
[8.3.1] Gestión de soportes extraíbles	L0-L3	L2-L3	L2-L3
[8.3.2] Retirada de soportes	L0-L2	L2	L2-L3
[8.3.3] Transferencia de soportes físicos	L0-L2	L1-L3	L2-L4

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[8] Gestión de activos	22%	55%	72%
[8.1] Responsabilidad sobre los activos	28%	62%	73%
[8.1.1] Inventario de activos	23%	52%	70%
[8.1.2] Propiedad de los activos	16%	50%	68%
[8.1.3] Uso aceptable de los activos	23%	54%	63%
[8.1.4] Devolución de activos	50%	90%	90%
[8.2] Clasificación de la información	12%	43%	73%
[8.2.1] Clasificación de la información	12%	30%	80%
[8.2.2] Marcado de la información	0%	30%	70%
[8.2.3] Manejo de activos	25%	70%	70%
[8.3] Manipulación de los soportes	24%	59%	70%
[8.3.1] Gestión de soportes extraíbles	38%	70%	70%
[8.3.2] Retirada de soportes	25%	50%	70%
[8.3.3] Transferencia de soportes físicos	10%	57%	71%

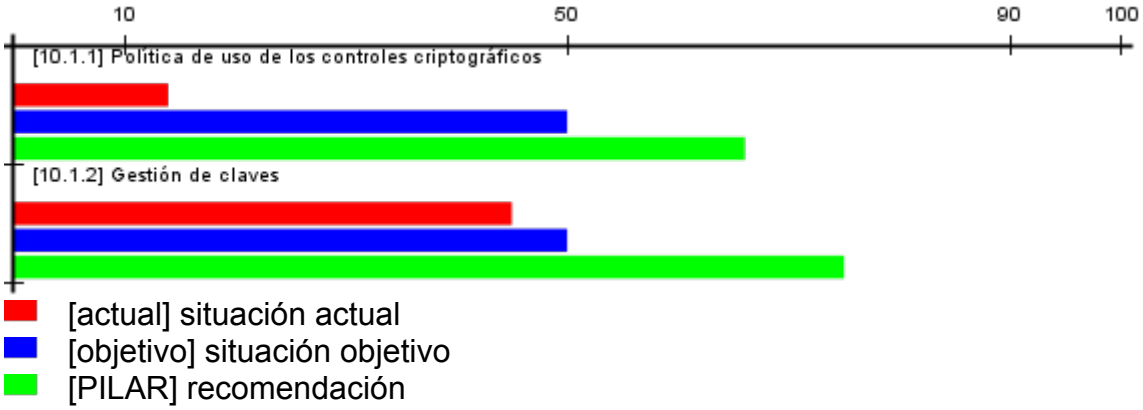
[9] Control de acceso



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[9] Control de acceso	L0-L3	L1-L4	L2-L5
[9.1] Requisitos de negocio para el control de acceso	L0-L3	L2-L3	L2-L3
[9.1.1] Política de control de acceso	L0-L3	L2-L3	L2-L3
[9.1.2] Acceso a redes y servicios en red	L1	L2	L2
[9.2] Gestión del acceso de usuario	L0-L3	L1-L4	L2-L4
[9.2.1] Altas y bajas de usuarios	L2-L3	L3	L3
[9.2.2] Gestión de derechos de acceso de los usuarios	L0-L2	L1-L3	L2-L3
[9.2.3] Gestión de derechos de acceso especiales	L0-L3	L1-L3	L2-L4
[9.2.4] Gestión de la información secreta de autenticación de usuarios	L0-L2	L2-L4	L2-L4
[9.2.5] Revisión de derechos de acceso de usuario	L0-L2	L2-L3	L3
[9.2.6] Terminación o revisión de los privilegios de acceso	L2	L3	L3
[9.3] Responsabilidades de usuario	L2	L4	L4
[9.3.1] Uso de la información secreta de autenticación	L2	L4	L4
[9.4] Control de acceso al sistema y a las aplicaciones	L0-L3	L1-L3	L2-L5
[9.4.1] Restricción del acceso a la información	L2	L2-L3	L2-L3
[9.4.2] Procedimientos seguros de inicio de sesión	L0-L3	L2-L3	L3-L5
[9.4.3] Gestión de las contraseñas de usuario	L0-L3	L2-L3	L2-L5
[9.4.4] Uso de los recursos del sistema con privilegios especiales	L0-L2	L1-L3	L3
[9.4.5] Control de acceso al código fuente de los programas	L0-L2	L1-L3	L2-L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[9] Control de acceso	39%	76%	83%
[9.1] Requisitos de negocio para el control de acceso	26%	65%	68%
[9.1.1] Política de control de acceso	43%	80%	85%
[9.1.2] Acceso a redes y servicios en red	10%	50%	50%
[9.2] Gestión del acceso de usuario	39%	75%	84%
[9.2.1] Altas y bajas de usuarios	65%	90%	90%
[9.2.2] Gestión de derechos de acceso de los usuarios	15%	53%	73%
[9.2.3] Gestión de derechos de acceso especiales	42%	67%	82%
[9.2.4] Gestión de la información secreta de autenticación de usuarios	38%	82%	81%
[9.2.5] Revisión de derechos de acceso de usuario	25%	70%	90%
[9.2.6] Terminación o revisión de los privilegios de acceso	50%	90%	90%
[9.3] Responsabilidades de usuario	50%	95%	95%
[9.3.1] Uso de la información secreta de autenticación	50%	95%	95%
[9.4] Control de acceso al sistema y a las aplicaciones	39%	67%	83%
[9.4.1] Restricción del acceso a la información	50%	80%	80%
[9.4.2] Procedimientos seguros de inicio de sesión	60%	77%	94%
[9.4.3] Gestión de las contraseñas de usuario	36%	77%	82%
[11.2.3.services] contraseñas de acceso a los servicios	50%	70%	92%
[11.2.3.sw] contraseñas de acceso a las aplicaciones	50%	70%	92%
[11.2.3.comms] contraseñas de acceso a los servicios de comunicaciones	90%	90%	95%
[9.4.4] Uso de los recursos del sistema con privilegios especiales	25%	50%	90%
[9.4.5] Control de acceso al código fuente de los programas	25%	50%	70%

[10] Criptografía

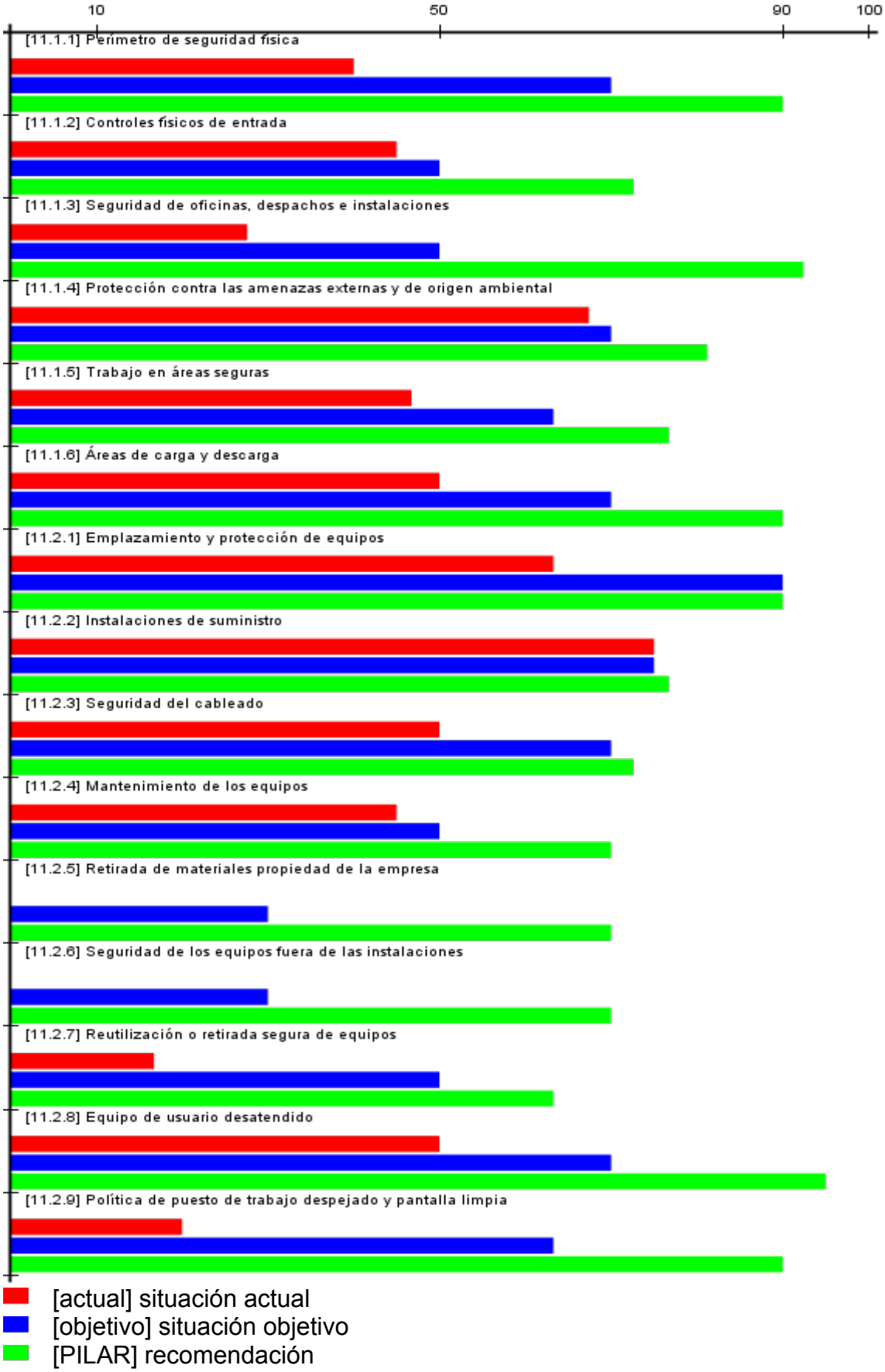


[actual] situación actual
[objetivo] situación objetivo
[PILAR] recomendación

Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[10] Criptografía	L0-L3	L1-L3	L2-L5
[10.1] Controles criptográficos	L0-L3	L1-L3	L2-L5
[10.1.1] Política de uso de los controles criptográficos	L0-L2	L2	L2-L3
[10.1.2] Gestión de claves	L0-L3	L1-L3	L2-L5

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[10] Criptografía	30%	50%	70%
[10.1] Controles criptográficos	30%	50%	70%
[10.1.1] Política de uso de los controles criptográficos	14%	50%	66%
[10.1.2] Gestión de claves	45%	50%	75%

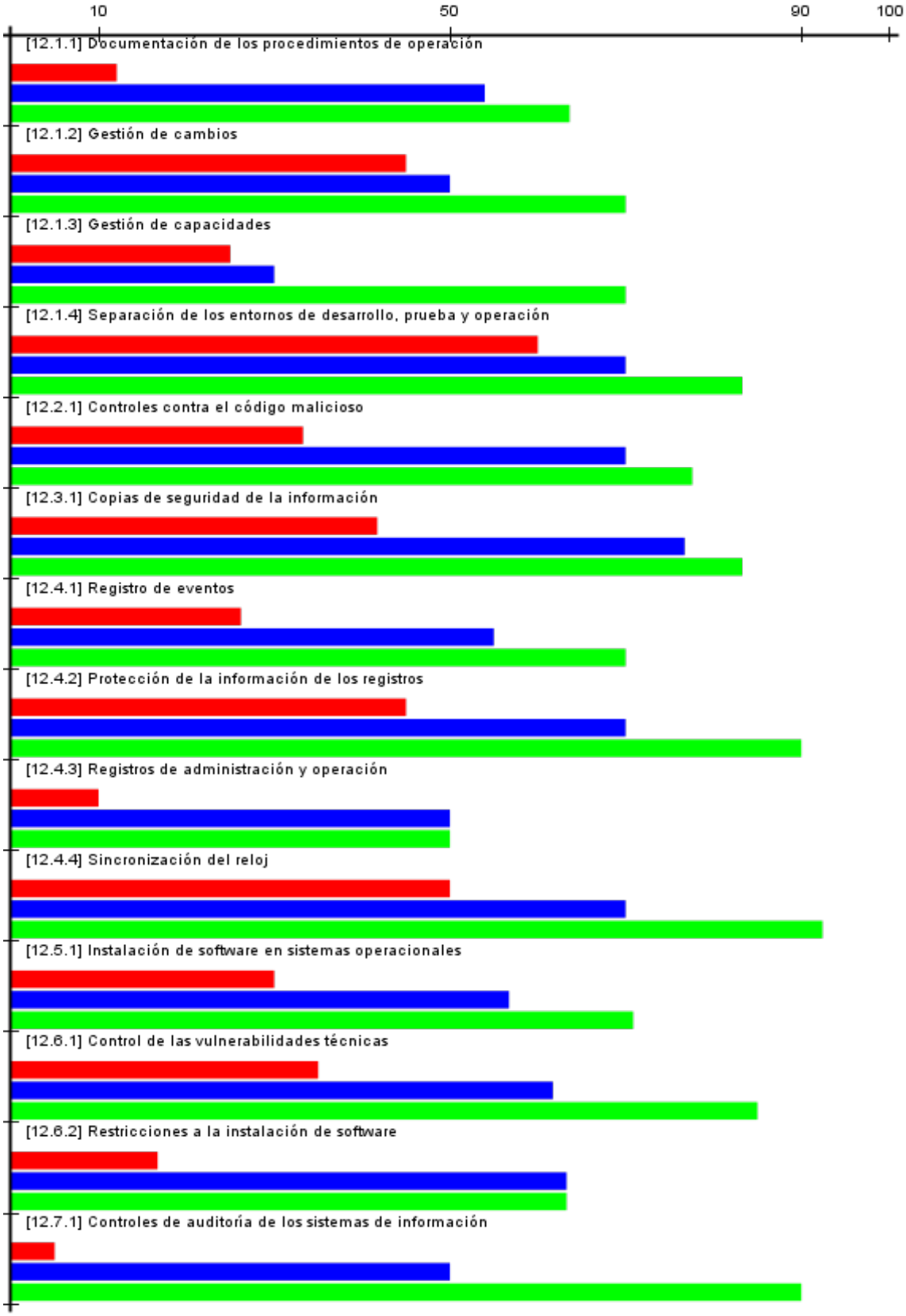
[11] Seguridad física y del entorno



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[11] Seguridad física y del entorno	L0-L3	L0-L3	L2-L5
[11.1] Áreas seguras	L0-L3	L1-L3	L2-L4
[11.1.1] Perímetro de seguridad física	L1-L2	L2-L3	L3
[11.1.2] Controles físicos de entrada	L0-L3	L1-L3	L2-L4
[11.1.3] Seguridad de oficinas, despachos e instalaciones	L0-L3	L1-L3	L3-L4
[11.1.4] Protección contra las amenazas externas y de origen ambiental	L0-L3	L1-L3	L2-L4
[11.1.5] Trabajo en áreas seguras	L0-L3	L1-L3	L2-L3
[11.1.6] Áreas de carga y descarga	L1-L3	L2-L3	L3
[11.2] Equipos	L0-L3	L0-L3	L2-L5
[11.2.1] Emplazamiento y protección de equipos	L2-L3	L3	L3
[11.2.2] Instalaciones de suministro	L0-L3	L0-L3	L2-L3
[11.2.3] Seguridad del cableado	L1-L3	L2-L3	L2-L4
[11.2.4] Mantenimiento de los equipos	L0-L3	L1-L3	L2-L3
[11.2.5] Retirada de materiales propiedad de la empresa	L0	L1-L2	L2-L3
[11.2.6] Seguridad de los equipos fuera de las instalaciones	L0	L1-L2	L2-L3
[11.2.7] Reutilización o retirada segura de equipos	L0-L2	L2	L2-L3
[11.2.8] Equipo de usuario desatendido	L1-L3	L2-L3	L3-L5
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	L0-L2	L2-L3	L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[11] Seguridad física y del entorno	41%	60%	81%
[11.1] Áreas seguras	46%	62%	84%
[11.1.1] Perímetro de seguridad física	40%	70%	90%
[11.1.2] Controles físicos de entrada	45%	50%	73%
[11.1.3] Seguridad de oficinas, despachos e instalaciones	28%	50%	92%
[11.1.4] Protección contra las amenazas externas y de origen ambiental	67%	70%	81%
[11.1.5] Trabajo en áreas seguras	47%	63%	77%
[11.1.6] Áreas de carga y descarga	50%	70%	90%
[11.2] Equipos	36%	59%	77%
[11.2.1] Emplazamiento y protección de equipos	63%	90%	90%
[11.2.2] Instalaciones de suministro	75%	75%	77%
[11.2.3] Seguridad del cableado	50%	70%	73%
[11.2.4] Mantenimiento de los equipos	45%	50%	70%
[11.2.5] Retirada de materiales propiedad de la empresa	0%	30%	70%
[11.2.6] Seguridad de los equipos fuera de las instalaciones	0%	30%	70%
[11.2.7] Reutilización o retirada segura de equipos	17%	50%	63%
[11.2.8] Equipo de usuario desatendido	50%	70%	95%
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	20%	63%	90%

[12] Gestión de operaciones

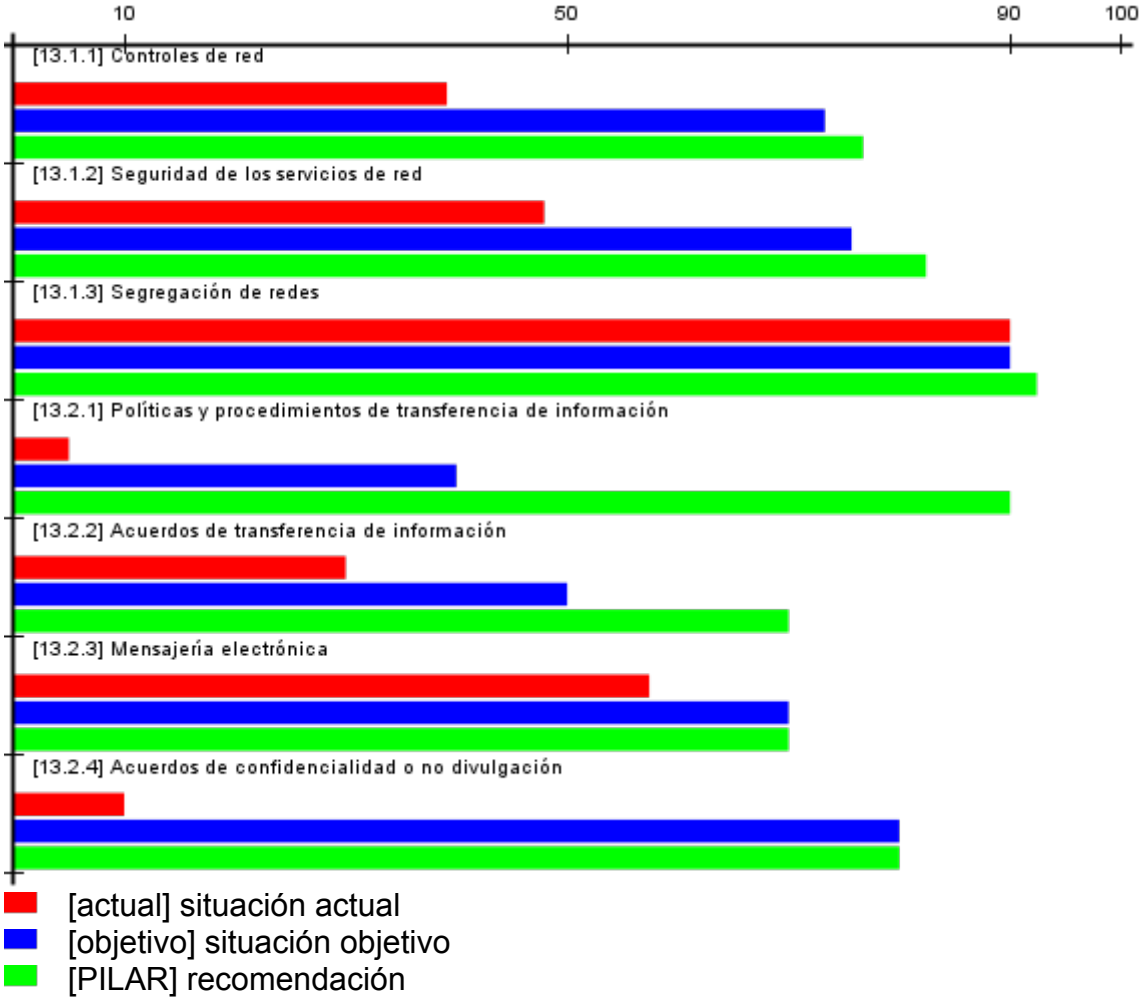


[actual] situación actual
[objetivo] situación objetivo
[PILAR] recomendación

Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[12] Gestión de operaciones	L0-L3	L0-L3	L2-L4
[12.1] Responsabilidades y procedimientos de operación	L0-L3	L1-L3	L2-L3
[12.1.1] Documentación de los procedimientos de operación	L0-L2	L2-L3	L2-L3
[12.1.2] Gestión de cambios	L0-L3	L1-L3	L2-L3
[12.1.3] Gestión de capacidades	L0-L2	L1-L2	L2-L3
[12.1.4] Separación de los entornos de desarrollo, prueba y operación	L0-L3	L1-L3	L2-L3
[12.2] Protección contra el código malicioso	L0-L3	L2-L3	L2-L4
[12.2.1] Controles contra el código malicioso	L0-L3	L2-L3	L2-L4
[12.3] Copias de seguridad	L0-L3	L2-L3	L2-L3
[12.3.1] Copias de seguridad de la información	L0-L3	L2-L3	L2-L3
[12.4] Registro y monitorización	L0-L3	L1-L3	L2-L4
[12.4.1] Registro de eventos	L0-L3	L1-L3	L2-L3
[12.4.2] Protección de la información de los registros	L0-L3	L2-L3	L3
[12.4.3] Registros de administración y operación	L1	L2	L2
[12.4.4] Sincronización del reloj	L1-L3	L2-L3	L3-L4
[12.5] Control del software en explotación	L0-L3	L1-L3	L2-L4
[12.5.1] Instalación de software en sistemas operacionales	L0-L3	L1-L3	L2-L4
[12.6] Gestión de las vulnerabilidades técnicas	L0-L3	L0-L3	L2-L4
[12.6.1] Control de las vulnerabilidades técnicas	L0-L3	L0-L3	L2-L4
[12.6.2] Restricciones a la instalación de software	L0-L2	L2-L3	L2-L3
[12.7] Consideraciones sobre la auditoría de los sistemas de información	L0-L1	L2	L3
[12.7.1] Controles de auditoría de los sistemas de información	L0-L1	L2	L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[12] Gestión de operaciones	29%	61%	78%
[12.1] Responsabilidades y procedimientos de operación	35%	51%	72%
[12.1.1] Documentación de los procedimientos de operación	12%	54%	64%
[12.1.2] Gestión de cambios	45%	50%	70%
[12.1.3] Gestión de capacidades	25%	30%	70%
[12.1.4] Separación de los entornos de desarrollo, prueba y operación	60%	70%	83%
[12.2] Protección contra el código malicioso	33%	70%	78%
[12.2.1] Controles contra el código malicioso	33%	70%	78%
[12.3] Copias de seguridad	42%	77%	83%
[12.3.1] Copias de seguridad de la información	42%	77%	83%
[12.4] Registro y monitorización	33%	61%	76%
[12.4.1] Registro de eventos	26%	55%	70%
[12.4.2] Protección de la información de los registros	45%	70%	90%
[12.4.3] Registros de administración y operación	10%	50%	50%
[12.4.4] Sincronización del reloj	50%	70%	92%
[12.5] Control del software en explotación	30%	57%	71%
[12.5.1] Instalación de software en sistemas operacionales	30%	57%	71%
[12.6] Gestión de las vulnerabilidades técnicas	26%	62%	74%
[12.6.1] Control de las vulnerabilidades técnicas	35%	62%	85%
[12.6.2] Restricciones a la instalación de software	17%	63%	63%
[12.7] Consideraciones sobre la auditoría de los sistemas de información	5%	50%	90%
[12.7.1] Controles de auditoría de los sistemas de información	5%	50%	90%

[13] Seguridad de las telecomunicaciones

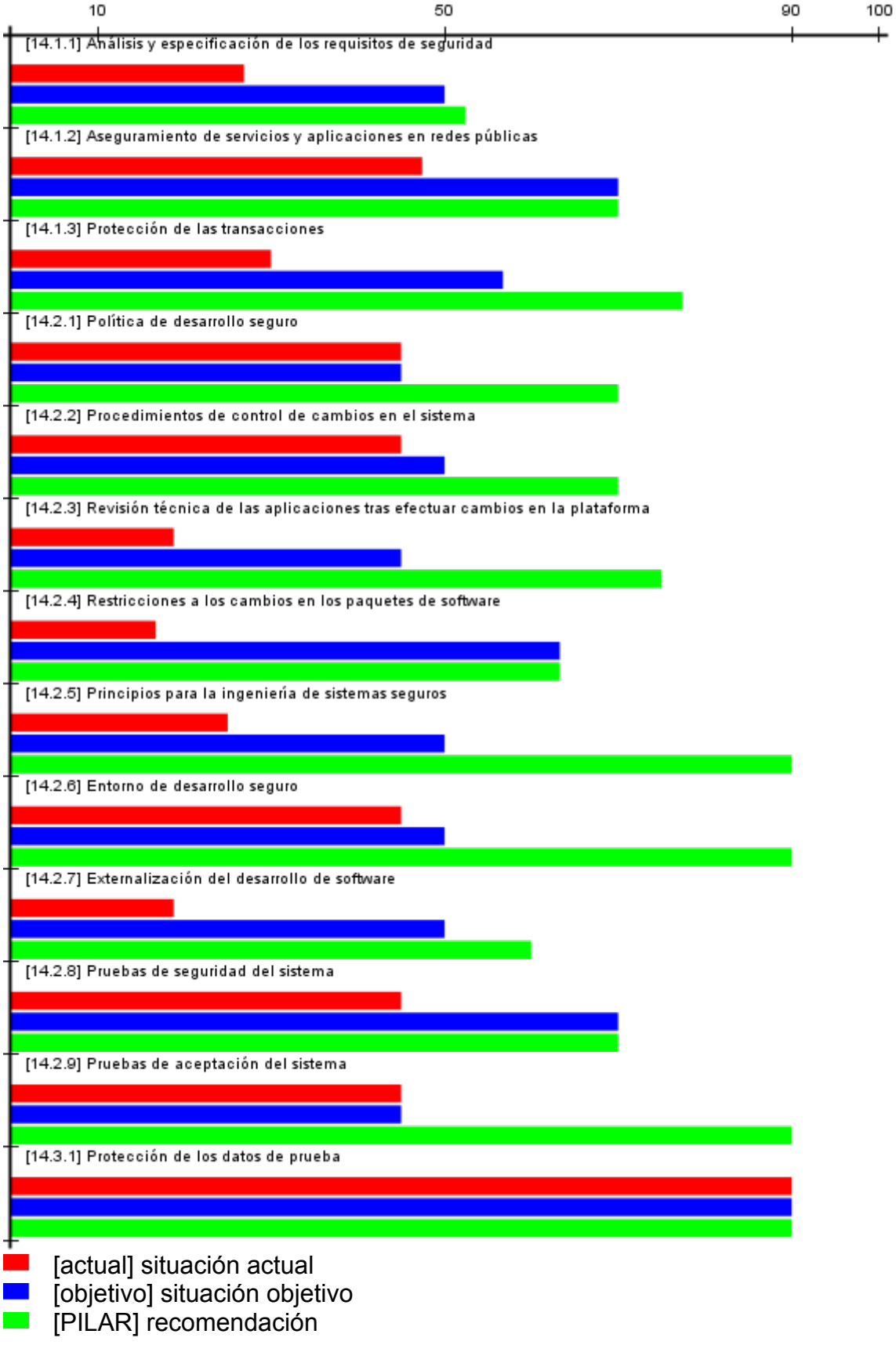


Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[13] Seguridad de las comunicaciones	L0-L3	L1-L3	L2-L5
[13.1] Gestión de la seguridad de las redes	L0-L3	L2-L3	L2-L5
[13.1.1] Controles de red	L0-L3	L2-L3	L2-L3
[13.1.2] Seguridad de los servicios de red	L0-L3	L2-L3	L2-L5
[13.1.3] Segregación de redes	L3	L3	L3-L4
[13.2] Transferencia de información	L0-L3	L1-L3	L2-L3
[13.2.1] Políticas y procedimientos de transferencia de información	L0-L1	L1-L2	L3
[13.2.2] Acuerdos de transferencia de información	L1-L2	L1-L3	L2-L3
[13.2.3] Mensajería electrónica	L0-L3	L2-L3	L2-L3
[13.2.4] Acuerdos de confidencialidad o no divulgación	L1	L2-L3	L2-L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[13] Seguridad de las comunicaciones	42%	70%	81%
[13.1] Gestión de la seguridad de las redes	59%	80%	84%
[13.1.1] Controles de red	39%	73%	77%
[13.1.2] Seguridad de los servicios de red	48%	76%	82%
[13.1.3] Segregación de redes	90%	90%	92%
[13.2] Transferencia de información	26%	60%	77%
[13.2.1] Políticas y procedimientos de transferencia de información	5%	40%	90%
[13.2.2] Acuerdos de transferencia de información	30%	50%	70%
[13.2.3] Mensajería electrónica	57%	70%	70%

[13.2.4] Acuerdos de confidencialidad o no divulgación	10%	80%	80%

[14] Adquisición, desarrollo y mantenimiento de los sistemas

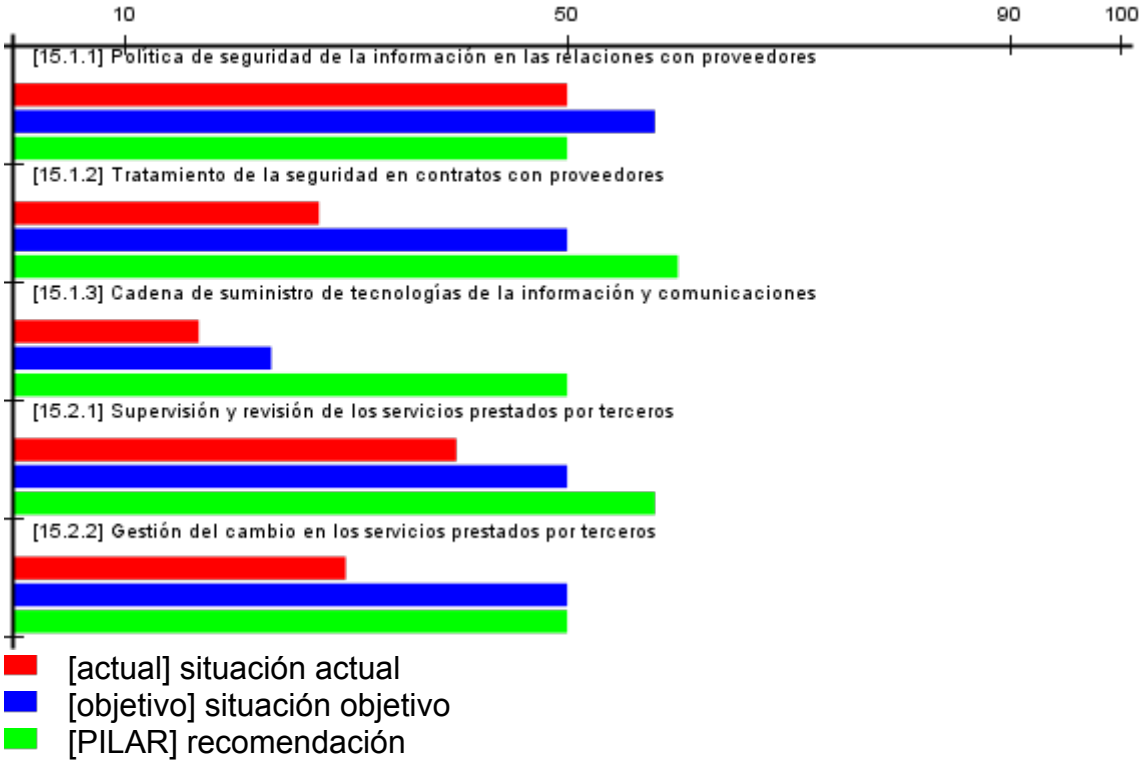


[14] Adquisición, desarrollo y mantenimiento de los sistemas

Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[14] Adquisición, desarrollo y mantenimiento de los sistemas	L0-L3	L0-L3	L2-L4
[14.1] Requisitos de seguridad de los sistemas de información	L0-L3	L1-L3	L2-L4
[14.1.1] Análisis y especificación de los requisitos de seguridad	L0-L2	L2	L2-L3
[14.1.2] Aseguramiento de servicios y aplicaciones en redes públicas	L0-L3	L2-L3	L2-L3
[14.1.3] Protección de las transacciones	L0-L3	L1-L3	L2-L4
[14.2] Seguridad en los procesos de desarrollo y soporte	L0-L3	L0-L3	L2-L3
[14.2.1] Política de desarrollo seguro	L0-L3	L0-L3	L2-L3
[14.2.2] Procedimientos de control de cambios en el sistema	L0-L3	L1-L3	L2-L3
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	L0-L2	L1-L3	L2-L3
[14.2.4] Restricciones a los cambios en los paquetes de software	L0-L2	L2-L3	L2-L3
[14.2.5] Principios para la ingeniería de sistemas seguros	L0-L2	L1-L3	L3
[14.2.6] Entorno de desarrollo seguro	L0-L3	L1-L3	L3
[14.2.7] Externalización del desarrollo de software	L0-L2	L1-L3	L2-L3
[14.2.8] Pruebas de seguridad del sistema	L0-L3	L2-L3	L2-L3
[14.2.9] Pruebas de aceptación del sistema	L0-L3	L0-L3	L3
[14.3] Datos de prueba	L3	L3	L3
[14.3.1] Protección de los datos de prueba	L3	L3	L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[14] Adquisición, desarrollo y mantenimiento de los sistemas	53%	67%	77%
[14.1] Requisitos de seguridad de los sistemas de información	35%	59%	67%
[14.1.1] Análisis y especificación de los requisitos de seguridad	27%	50%	52%
[14.1.2] Aseguramiento de servicios y aplicaciones en redes públicas	47%	70%	70%
[14.1.3] Protección de las transacciones	30%	57%	77%
[14.2] Seguridad en los procesos de desarrollo y soporte	34%	52%	75%
[14.2.1] Política de desarrollo seguro	45%	45%	70%
[14.2.2] Procedimientos de control de cambios en el sistema	45%	50%	70%
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	19%	45%	75%
[14.2.4] Restricciones a los cambios en los paquetes de software	17%	63%	63%
[14.2.5] Principios para la ingeniería de sistemas seguros	25%	50%	90%
[14.2.6] Entorno de desarrollo seguro	45%	50%	90%
[14.2.7] Externalización del desarrollo de software	19%	50%	60%
[14.2.8] Pruebas de seguridad del sistema	45%	70%	70%
[14.2.9] Pruebas de aceptación del sistema	45%	45%	90%
[14.3] Datos de prueba	90%	90%	90%
[14.3.1] Protección de los datos de prueba	90%	90%	90%

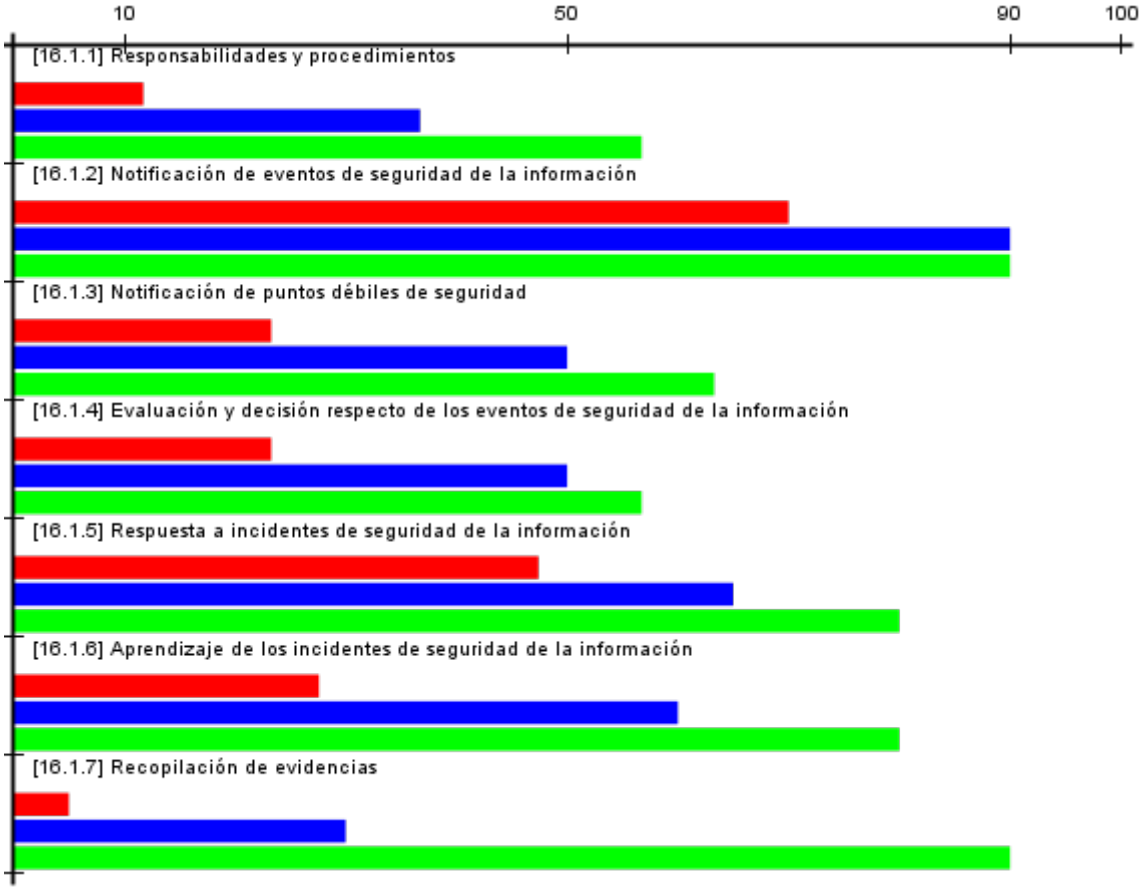
[15] Relaciones con proveedores



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[15] Relaciones con proveedores	L0-L3	L1-L3	L2-L3
[15.1] Seguridad de la información en las relaciones con proveedores	L0-L3	L1-L3	L2-L3
[15.1.1] Política de seguridad de la información en las relaciones con proveedores	L1-L3	L2-L3	L2
[15.1.2] Tratamiento de la seguridad en contratos con proveedores	L0-L3	L1-L3	L2-L3
[15.1.3] Cadena de suministro de tecnologías de la información y comunicaciones	L0-L2	L1-L2	L2
[15.2] Gestión de servicios prestados por terceros	L0-L3	L1-L3	L2-L3
[15.2.1] Supervisión y revisión de los servicios prestados por terceros	L0-L3	L1-L3	L2-L3
[15.2.2] Gestión del cambio en los servicios prestados por terceros	L1-L2	L2	L2

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[15] Relaciones con proveedores	33%	47%	54%
[15.1] Seguridad de la información en las relaciones con proveedores	31%	44%	53%
[15.1.1] Política de seguridad de la información en las relaciones con proveedores	50%	58%	50%
[15.1.2] Tratamiento de la seguridad en contratos con proveedores	28%	50%	60%
[15.1.3] Cadena de suministro de tecnologías de la información y comunicaciones	17%	23%	50%
[15.2] Gestión de servicios prestados por terceros	35%	50%	54%
[15.2.1] Supervisión y revisión de los servicios prestados por terceros	40%	50%	58%
[15.2.2] Gestión del cambio en los servicios prestados por terceros	30%	50%	50%

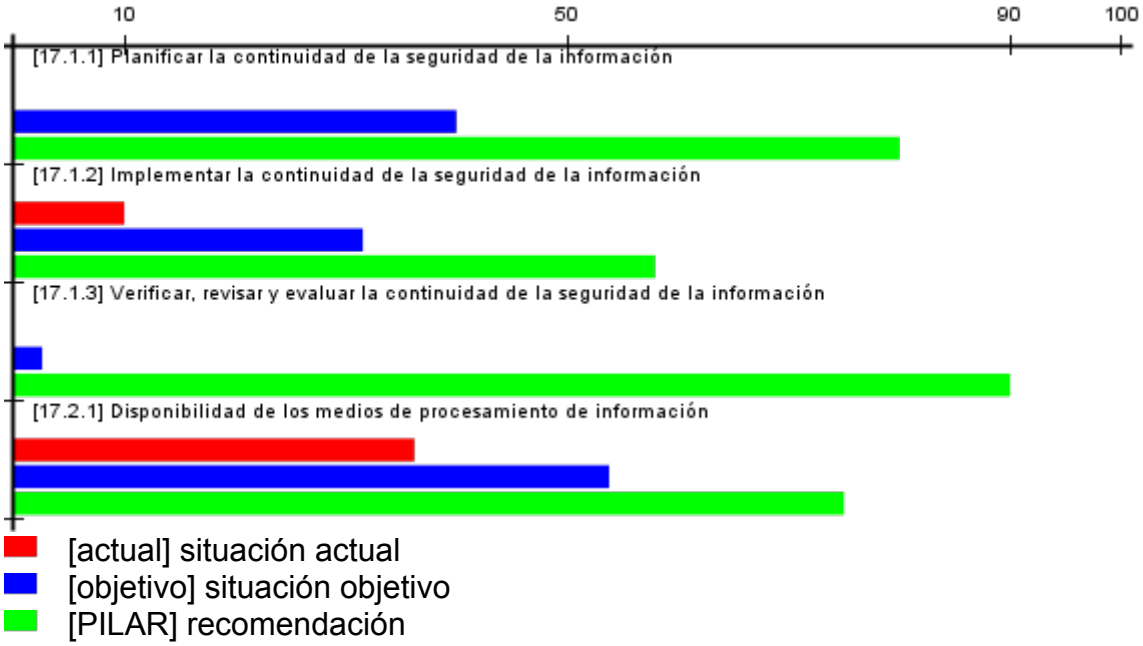
[16] Gestión de incidentes de seguridad de la información



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[16] Gestión de incidentes de seguridad de la información	L0-L3	L1-L3	L2-L3
[16.1] Gestión de incidentes de seguridad de la información y mejoras	L0-L3	L1-L3	L2-L3
[16.1.1] Responsabilidades y procedimientos	L0-L2	L1-L3	L2-L3
[16.1.2] Notificación de eventos de seguridad de la información	L2-L3	L3	L3
[16.1.3] Notificación de puntos débiles de seguridad	L1-L2	L2	L2-L3
[16.1.4] Evaluación y decisión respecto de los eventos de seguridad de la información	L1-L2	L2	L2-L3
[16.1.5] Respuesta a incidentes de seguridad de la información	L0-L3	L1-L3	L2-L3
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	L0-L2	L1-L3	L2-L3
[16.1.7] Recopilación de evidencias	L0-L1	L1-L2	L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[16] Gestión de incidentes de seguridad de la información	30%	55%	74%
[16.1] Gestión de incidentes de seguridad de la información y mejoras	30%	55%	74%
[16.1.1] Responsabilidades y procedimientos	12%	37%	57%
[16.1.2] Notificación de eventos de seguridad de la información	70%	90%	90%
[16.1.3] Notificación de puntos débiles de seguridad	23%	50%	63%
[16.1.4] Evaluación y decisión respecto de los eventos de seguridad de la información	23%	50%	57%
[16.1.5] Respuesta a incidentes de seguridad de la información	47%	65%	80%
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	28%	60%	80%
[16.1.7] Recopilación de evidencias	5%	30%	90%

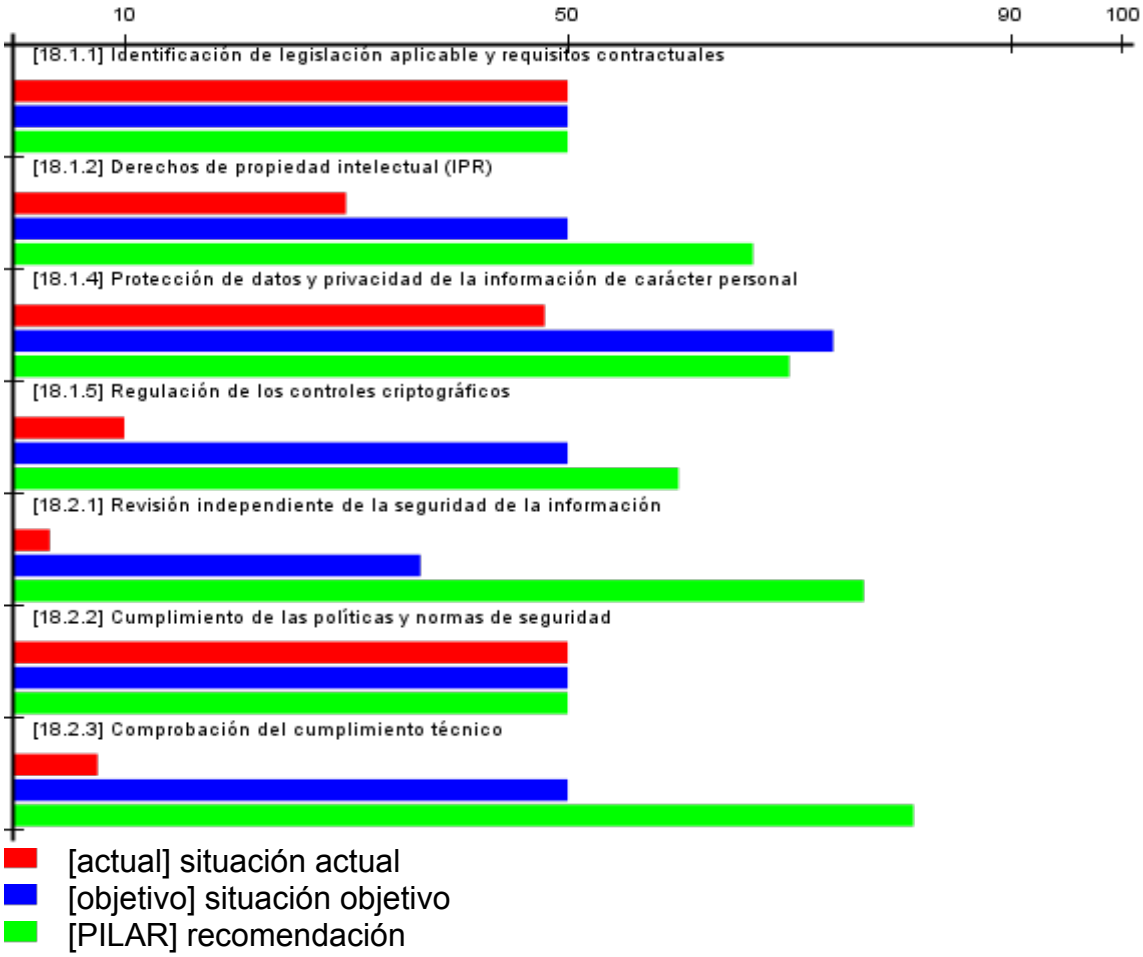
[17] Aspectos de la seguridad de la información en la gestión de la continuidad del negocio



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	L0-L3	L0-L3	L2-L3
[17.1] Continuidad de la seguridad de la información	L0-L3	L0-L3	L2-L3
[17.1.1] Planificar la continuidad de la seguridad de la información	L0	L1-L2	L2-L3
[17.1.2] Implementar la continuidad de la seguridad de la información	L0-L3	L0-L3	L2-L3
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	L0	L0-L1	L3
[17.2] Redundancia	L0-L3	L0-L3	L2-L3
[17.2.1] Disponibilidad de los medios de procesamiento de información	L0-L3	L0-L3	L2-L3

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	20%	39%	75%
[17.1] Continuidad de la seguridad de la información	3%	25%	76%
[17.1.1] Planificar la continuidad de la seguridad de la información	0%	40%	80%
[17.1.2] Implementar la continuidad de la seguridad de la información	10%	31%	58%
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	0%	3%	90%
[17.2] Redundancia	36%	54%	75%
[17.2.1] Disponibilidad de los medios de procesamiento de información	36%	54%	75%

[18] Cumplimiento



Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[18] Cumplimiento	L0-L3	L1-L3	L2-L4
[18.1] Cumplimiento de los requisitos legales y contractuales	L0-L3	L2-L3	L2-L3
[18.1.1] Identificación de legislación aplicable y requisitos contractuales	L2	L2	L2
[18.1.2] Derechos de propiedad intelectual (IPR)	L1-L2	L2	L2-L3
[18.1.4] Protección de datos y privacidad de la información de carácter personal	L0-L3	L2-L3	L2-L3
[18.1.5] Regulación de los controles criptográficos	L1	L2	L2-L3
[18.2] Revisiones de seguridad de la información	L0-L2	L1-L3	L2-L4
[18.2.1] Revisión independiente de la seguridad de la información	L0-L1	L1-L2	L2-L3
[18.2.2] Cumplimiento de las políticas y normas de seguridad	L2	L2	L2
[18.2.3] Comprobación del cumplimiento técnico	L0-L1	L1-L3	L2-L4

Percentatge	**[actual]**	**[objetivo]**	**[PILAR]**
[18] Cumplimiento	27%	51%	65%
[18.1] Cumplimiento de los requisitos legales y contractuales	34%	56%	62%
[18.1.1] Identificación de legislación aplicable y requisitos contractuales	50%	50%	50%
[18.1.2] Derechos de propiedad intelectual (IPR)	30%	50%	67%
[18.1.4] Protección de datos y privacidad de la información de carácter personal	48%	74%	70%
[18.1.5] Regulación de los controles criptográficos	10%	50%	60%
[18.2] Revisiones de seguridad de la información	20%	46%	69%
[18.2.1] Revisión independiente de la seguridad de la información	3%	37%	77%
[18.2.2] Cumplimiento de las políticas y normas de seguridad	50%	50%	50%
[18.2.3] Comprobación del cumplimiento técnico	8%	50%	81%

Annex V – Informe declaració aplicabilitat PILAR

Informe de declaració d'aplicabilitat extret de l'eina PILAR.

ISO/IEC 27002:2013

Declaración de Aplicabilidad

[2700AJFITA] 2700-Aj_FitaAlta

27.4.2016

3 Introducción

Código: 2700AJFITA
Nombre: 2700-Aj_FitaAlta
Descripción:

> Anàlisi de riscos seguint la metodologia MAGERIT utilitzant l'aplicació micro Pilar per al treball de fi de Màster de la UOC amb l'organització fictícia "Ajuntament de Fita Alta"

Datos administrativos:

- desc: Anàlisi de Riscos de l'Ajuntament de Fita Alta -
- resp: Andreu Retamero Pallarès
- org: Ajuntament de Fita Alta
- ver: 1.0
- date: 12/04/2016

Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

4 Valoración del sistema

essential

activo	[D]	[I]	[C]	[A]	[T]
[NOT-ELEC] Notificacions telemàtiques	[1](1)	[4]	[4]	[4]	[4]
[VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4](2)
[INFOPUB] Informació pública	[1](3)	[4](4)	[0](5)	[4]	[0]
[CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
[CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
[TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
[IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
[POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]
[LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]

(1) [1.da] Pudiera causar la interrupción de actividades propias de la Organización
(2) [cei] Intereses Comerciales / Económicos:
(3) Informació publica: calendari contribuent, ordenances, extractes dels acords de la JG, reglaments.. La no disponibilitat d'aquesta informació no suposa cap interrupció de servei, ni afecta a la productivitat i es pot obtenir per un altre canal (presencial o telefònic)
(4) La manipulació de la informació pública no causaria pèrdues econòmiques però si danys en la imatge de l'ajuntament davant tercers.
[b] por afectar gravemente a las relaciones con el público en general
(5) La informació és pública

5 ISO/IEC 27002:2013

5.3 [5] Políticas de seguridad de la información

[base] Base

control	aplicable
[5] Políticas de seguridad de la información	sí
[5.1] Dirección de la gestión de la seguridad de la información	sí
[5.1.1] Políticas de seguridad de la información	sí
[5.1.2] Revisión de las políticas de seguridad de la información	sí

5.4 [6] Organización de la seguridad de la información

[base] Base

control	aplicable
[6] Organización de la seguridad de la información	sí
[6.1] Organización interna	sí
[6.1.1] Roles y responsabilidades relativas a la seguridad de la información	sí
[6.1.2] Separación de tareas	sí
[6.1.3] Contacto con las autoridades	sí

[6.1.4] Contacto con grupos de especial interés	sí
[6.1.5] Seguridad de la información en la gestión de proyectos	sí
[6.2] Dispositivos móviles y teletrabajo	sí
[6.2.1] Política de dispositivos móviles	sí
[6.2.2] Teletrabajo	sí

5.5 [7] Seguridad ligada a los recursos humanos

[base] Base

control	aplicable
[7] Seguridad ligada a los recursos humanos	sí
[7.1] Antes del empleo	sí
[7.1.1] Investigación de antecedentes	sí
[7.1.2] Términos y condiciones de contratación	sí
[7.2] Durante el empleo	sí
[7.2.1] Responsabilidades de la Dirección	sí
[7.2.2] Concienciación, formación y capacitación en seguridad de la información	sí
[7.2.3] Proceso disciplinario	sí
[7.3] Cese del empleo o cambio de puesto de trabajo	sí
[7.3.1] Terminación o cambio de responsabilidades laborales	sí

5.6 [8] Gestión de activos

[base] Base

control	aplicable
[8] Gestión de activos	sí
[8.1] Responsabilidad sobre los activos	sí
[8.1.1] Inventario de activos	sí
[8.1.2] Propiedad de los activos	sí
[8.1.3] Uso aceptable de los activos	sí
[8.1.4] Devolución de activos	sí
[8.2] Clasificación de la información	sí
[8.2.1] Clasificación de la información	sí
[8.2.2] Marcado de la información	sí
[8.2.3] Manejo de activos	sí
[8.3] Manipulación de los soportes	sí
[8.3.1] Gestión de soportes extraíbles	sí
[8.3.2] Retirada de soportes	sí
[8.3.3] Transferencia de soportes físicos	sí

5.7 [9] Control de acceso

[base] Base

control	aplicable

[9] Control de acceso	sí
[9.1] Requisitos de negocio para el control de acceso	sí
[9.1.1] Política de control de acceso	sí
[9.1.2] Acceso a redes y servicios en red	sí
[9.2] Gestión del acceso de usuario	sí
[9.2.1] Altas y bajas de usuarios	sí
[9.2.2] Gestión de derechos de acceso de los usuarios	sí
[9.2.3] Gestión de derechos de acceso especiales	sí
[9.2.4] Gestión de la información secreta de autenticación de usuarios	sí
[9.2.5] Revisión de derechos de acceso de usuario	sí
[9.2.6] Terminación o revisión de los privilegios de acceso	sí
[9.3] Responsabilidades de usuario	sí
[9.3.1] Uso de la información secreta de autenticación	sí
[9.4] Control de acceso al sistema y a las aplicaciones	sí
[9.4.1] Restricción del acceso a la información	sí
[9.4.2] Procedimientos seguros de inicio de sesión	sí
[9.4.3] Gestión de las contraseñas de usuario	sí
[9.4.4] Uso de los recursos del sistema con privilegios especiales	sí
[9.4.5] Control de acceso al código fuente de los programas	sí

5.8 [10] Criptografía

[base] Base

control	aplicable
[10] Criptografía	sí
[10.1] Controles criptográficos	sí
[10.1.1] Política de uso de los controles criptográficos	sí
[10.1.2] Gestión de claves	sí

5.9 [11] Seguridad física y del entorno

[base] Base

control	aplicable
[11] Seguridad física y del entorno	sí
[11.1] Áreas seguras	sí
[11.1.1] Perímetro de seguridad física	sí
[11.1.2] Controles físicos de entrada	sí
[11.1.3] Seguridad de oficinas, despachos e instalaciones	sí
[11.1.4] Protección contra las amenazas externas y de origen ambiental	sí
[11.1.5] Trabajo en áreas seguras	sí
[11.1.6] Áreas de carga y descarga	sí
[11.2] Equipos	sí
[11.2.1] Emplazamiento y protección de equipos	sí
[11.2.2] Instalaciones de suministro	sí
[11.2.3] Seguridad del cableado	sí
[11.2.4] Mantenimiento de los equipos	sí

[11.2.5] Retirada de materiales propiedad de la empresa	sí
[11.2.6] Seguridad de los equipos fuera de las instalaciones	sí
[11.2.7] Reutilización o retirada segura de equipos	sí
[11.2.8] Equipo de usuario desatendido	sí
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	sí

5.10 [12] Gestión de operaciones

[base] Base

control	aplicable
[12] Gestión de operaciones	sí
[12.1] Responsabilidades y procedimientos de operación	sí
[12.1.1] Documentación de los procedimientos de operación	sí
[12.1.2] Gestión de cambios	sí
[12.1.3] Gestión de capacidades	sí
[12.1.4] Separación de los entornos de desarrollo, prueba y operación	sí
[12.2] Protección contra el código malicioso	sí
[12.2.1] Controles contra el código malicioso	sí
[12.3] Copias de seguridad	sí
[12.3.1] Copias de seguridad de la información	sí
[12.4] Registro y monitorización	sí
[12.4.1] Registro de eventos	sí
[12.4.2] Protección de la información de los registros	sí
[12.4.3] Registros de administración y operación	sí
[12.4.4] Sincronización del reloj	sí
[12.5] Control del software en explotación	sí
[12.5.1] Instalación de software en sistemas operacionales	sí
[12.6] Gestión de las vulnerabilidades técnicas	sí
[12.6.1] Control de las vulnerabilidades técnicas	sí
[12.6.2] Restricciones a la instalación de software	sí
[12.7] Consideraciones sobre la auditoría de los sistemas de información	sí
[12.7.1] Controles de auditoría de los sistemas de información	sí

5.11 [13] Seguridad de las telecomunicaciones

[base] Base

control	aplicable
[13] Seguridad de las comunicaciones	sí
[13.1] Gestión de la seguridad de las redes	sí
[13.1.1] Controles de red	sí
[13.1.2] Seguridad de los servicios de red	sí
[13.1.3] Segregación de redes	sí
[13.2] Transferencia de información	sí
[13.2.1] Políticas y procedimientos de transferencia de información	sí
[13.2.2] Acuerdos de transferencia de información	sí
[13.2.3] Mensajería electrónica	sí
[13.2.4] Acuerdos de confidencialidad o no divulgación	sí

5.12 [14] Adquisición, desarrollo y mantenimiento de los sistemas

[base] Base

control	aplicable
[14] Adquisición, desarrollo y mantenimiento de los sistemas	sí
[14.1] Requisitos de seguridad de los sistemas de información	sí
[14.1.1] Análisis y especificación de los requisitos de seguridad	sí
[14.1.2] Aseguramiento de servicios y aplicaciones en redes públicas	sí
[14.1.3] Protección de las transacciones	sí
[14.2] Seguridad en los procesos de desarrollo y soporte	sí
[14.2.1] Política de desarrollo seguro	sí
[14.2.2] Procedimientos de control de cambios en el sistema	sí
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	sí
[14.2.4] Restricciones a los cambios en los paquetes de software	sí
[14.2.5] Principios para la ingeniería de sistemas seguros	sí
[14.2.6] Entorno de desarrollo seguro	sí
[14.2.7] Externalización del desarrollo de software	sí
[14.2.8] Pruebas de seguridad del sistema	sí
[14.2.9] Pruebas de aceptación del sistema	sí
[14.3] Datos de prueba	sí
[14.3.1] Protección de los datos de prueba	sí

5.13 [15] Relaciones con proveedores

[base] Base

control	aplicable
[15] Relaciones con proveedores	sí
[15.1] Seguridad de la información en las relaciones con proveedores	sí
[15.1.1] Política de seguridad de la información en las relaciones con proveedores	sí
[15.1.2] Tratamiento de la seguridad en contratos con proveedores	sí
[15.1.3] Cadena de suministro de tecnologías de la información y comunicaciones	sí
[15.2] Gestión de servicios prestados por terceros	sí
[15.2.1] Supervisión y revisión de los servicios prestados por terceros	sí
[15.2.2] Gestión del cambio en los servicios prestados por terceros	sí

5.14 [16] Gestión de incidentes de seguridad de la información

[base] Base

control	aplicable
[16] Gestión de incidentes de seguridad de la información	sí
[16.1] Gestión de incidentes de seguridad de la información y mejoras	sí
[16.1.1] Responsabilidades y procedimientos	sí
[16.1.2] Notificación de eventos de seguridad de la información	sí
[16.1.3] Notificación de puntos débiles de seguridad	sí

[16.1.4] Evaluación y decisión respecto de los eventos de seguridad de la información	sí
[16.1.5] Respuesta a incidentes de seguridad de la información	sí
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	sí
[16.1.7] Recopilación de evidencias	sí

5.15 [17] Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

[base] Base

control	aplicable
[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	sí
[17.1] Continuidad de la seguridad de la información	sí
[17.1.1] Planificar la continuidad de la seguridad de la información	sí
[17.1.2] Implementar la continuidad de la seguridad de la información	sí
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	sí
[17.2] Redundancia	sí
[17.2.1] Disponibilidad de los medios de procesamiento de información	sí

5.16 [18] Cumplimiento

[base] Base

control	aplicable
[18] Cumplimiento	sí
[18.1] Cumplimiento de los requisitos legales y contractuales	sí
[18.1.1] Identificación de legislación aplicable y requisitos contractuales	sí
[18.1.2] Derechos de propiedad intelectual (IPR)	sí
[18.1.3] Protección de los documentos de la organización	n.a.
[18.1.4] Protección de datos y privacidad de la información de carácter personal	sí
[18.1.5] Regulación de los controles criptográficos	sí
[18.2] Revisiones de seguridad de la información	sí
[18.2.1] Revisión independiente de la seguridad de la información	sí
[18.2.2] Cumplimiento de las políticas y normas de seguridad	sí
[18.2.3] Comprobación del cumplimiento técnico	sí

Annex VI – Salvaguardes PILAR

Relació de Salvaguardes extretes de l'eina PILAR.

- [AUX.power.6.4.3] Acometida redundante (dos suministradores)
- [H.VM.5.1] Las pruebas de penetración se aplican a los controles de seguridad física
- [PS.cont.3.1] Otro personal propio con formación de urgencia
- [S.3.3.a] Se establece un protocolo específico de reacción frente a código dañino
- [S.3.3.4] Se establecen controles de protección física
- [K.comms.a.6] Se controla el acceso a las claves
- [NEW.SW.5.2] Los desarrolladores cambian regularmente de asignaciones
- [H.VM.5.d] Se realizan pruebas cuando se actualiza el software de base
- [H.VM.5.e] Se realizan pruebas cuando se despliegan nuevos servidores y servicios www
- [H.VM.5.f] Se realizan pruebas cuando se conecta el sistema a nuevas redes
- [PS.cont.3.2] Otro personal propio ya formado
- [PS.cont.3.3] Contrato con proveedor de recursos humanos
- [L.9] La seguridad de la instalación no es responsabilidad de un único guarda
- [L.7.4.4] Se mantienen contactos periódicos con los responsables de las fuerzas de apoyo exterior
- [PS.8.3] frente a extorsión
- [PS.8.2] frente a phishing
- [PS.8.4] frente a ataques de ingeniería social
- [L.7.7.4] Las actividades o misiones críticas se llevan a cabo lejos de cualquier punto vulnerable
- [BC.DRP.5.9] Está previsto personal alternativo
- [BC.DRP.5.a] Están previstos los lugares alternativos de trabajo
- [S.3.3.3] Se activan los servicios de registro de actividad
- [H.IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros
- [H.AC.7.7] Se separan las responsabilidades de administración y operación
- [PS.5.1.4] Se requiere una habilitación de seguridad de acuerdo al grado de clasificación de la información que se maneja
- [G.exam.4.3] Se planifica la reparación de los defectos descubiertos que implican un riesgo bajo
- [S.TW.9.4.1] Control de acceso como administrador
- [SW.start.6] Se verifica el funcionamiento de los registros de actividad
- [E.1.b] Se garantiza la integridad de la información

- [K.comms.a.9] Se retienen copias de los certificados de las claves
- [L.7.7.2] Se mantienen contactos con las Fuerzas y Cuerpos de Seguridad del Estado para conocer el nivel de alerta o de amenaza
- [L.7.7.5] Los puntos vulnerables de la instalación han sido identificados por personal experto en la materia
- [K.comms.a.5] Se protegen los medios de almacenamiento
- [COM.CM.d] Pruebas de regresión
- [S.start.6] Se lleva a cabo una campaña de ejecución de pruebas de regresión (para asegurarse de que no afecta a los demás servicios)
- [D.TS.6.1] Se utiliza firma electrónica de la autoridad de fechado (ISO:18014-2/1 / RFC 3161)
- [L.AC.2.9.1] de forma aleatoria
- [L.AC.2.a.1] de forma aleatoria
- [L.AC.b] Se prohíben equipos de registro (fotografía, video, audio, telefonía, etc.) salvo autorización especial
- [L.7.7.3] Se dispone de medios técnicos para la detección de metales y explosivos
- [L.design.6.1] muros
- [L.design.6.2] puertas
- [L.design.6.3] techos
- [L.design.6.4] suelo
- [S.op.1.1] Se requiere confirmación de envío
- [S.op.1.2] Se requiere confirmación de entrega
- [S.TW.9.4.2] Control de acceso como usuario normal
- [S.TW.9.4.3] Fortificación del equipo (bastionado)
- [S.TW.9.5] Instalación de software por parte de los usuarios
- [SW.CM.f] Pruebas de regresión
- [HW.CM.e] Pruebas de regresión
- [HW.PCD.8.1] Se han determinado las medidas para la protección física del dispositivo
- [HW.PCD.8.3] Se han establecido los requisitos sobre control de acceso
- [HW.PCD.8.4] Se utiliza un sistema de defensa perimetral (cortafuegos)
- [HW.PCD.8.5.1] Se cifra la información importante almacenada localmente
- [HW.PCD.8.5.2] No se almacenan en claro claves de acceso remoto
- [PS.cont.1] Se prevé suficiente holgura en el dimensionamiento de los equipos de trabajo
- [NEW.SW.5.9.2] La inspección la realiza un experto independiente
- [L.AC.2.9.2] de forma sistemática
- [L.AC.2.a.2] de forma sistemática
- [NEW.SW.5.4.3] Las herramientas de desarrollo no son accesibles al personal de producción
- [E.1.a] Se garantiza la confidencialidad de la información
- [E.1.e] Se establecen controles para asegurar la destrucción de la información cuando se requiera
- [K.comms.a.7] Se retienen copias de las claves de cifra

- [K.comms.a.8] Se retienen copias de las claves de descifrado
- [SW.start.5] Se verifica el funcionamiento de los controles de seguridad
- [COM.CM.g] Se actualizan todos los procedimientos de producción afectados
- [BC.DRP.5.3] Se han previsto los recursos necesarios
- [K.comms.4.2] Se sustituyen las claves comprometidas
- [S.TW.9.1] Se analiza la seguridad física
- [S.TW.9.2] Se analiza el entorno
- [S.TW.9.3] Se previene el uso del puesto por otras personas (acceso no autorizado)
- [S.TW.9.4.4] Anti virus
- [S.TW.9.4.5] Cortafuegos personal
- [S.TW.9.6] Seguridad de las comunicaciones
- [S.TW.9.7] Conexión a redes particulares por parte de los usuarios
- [SW.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
- [NEW.SW.5.1.3] Se contempla la posibilidad de inspeccionar el código fuente
- [NEW.SW.5.9.1.1] Puertas traseras
- [NEW.SW.5.9.1.2] Código troyano
- [NEW.SW.5.9.1.3] Canales encubiertos
- [NEW.SW.5.9.1.4] Desbordamiento (overflow)
- [NEW.SW.5.9.1.5] Escalado de privilegios
- [NEW.SW.5.4.2] Hay una separación de funciones entre el personal que desarrolla y el personal encargado de producción
- [H.ST.2.8] Administración de cambios
- [H.ST.2.9] Auditoría de seguridad
- [COM.SC.6] Se aplica la regla de 'seguridad por defecto'
- [H.IA.6.2.2] Las contraseñas se modifican al ser comprometidas o existir sospecha de ello
- [K.comms.4.3] Se sustituyen las claves bajo sospecha
- [H.IR.5.1] Se suspenden cautelarmente los trabajos en el sistema afectado
- [H.IR.2.5] Actuación frente a violaciones de la confidencialidad
- [K.comms.8.1] Almacén software con control de acceso
- [MP.IC.3] Se cifra el contenido
- [S.3.3.2] Se establecen controles para proteger la información
- [H.IR.2.4] Actuación ante errores que resulten de datos del negocio inexactos o incompletos
- [MP.4.3.6.4] Fraccionamiento del envío por rutas diferentes
- [H.IR.4.1] Se previene la fuga de información
- [H.IR.4.2] Se garantiza la integridad de la información
- [H.IR.4.3] Se previenen daños colaterales sobre otros sistemas
- [H.IR.4.4] Se previenen daños colaterales sobre personas afectadas
- [COM.aut.4.2.2.1] Los certificados se revocan al ser comprometidos o existir sospecha de ello

- [H.IR.2.c] Detección y reacción frente a actividades de espionaje industrial
- [H.VM.5.2] Las pruebas de penetración se aplican a los controles de seguridad lógica
- [H.VM.5.4] Se prueba a través de accesos WiFi
- [H.VM.5.5] Se prueba desde dentro (atacantes internos)
- [H.VM.5.6] Se realizan pruebas a nivel de red (network testing)
- [H.VM.5.8] Se incluyen pruebas de picaresca (social engineering)
- [H.VM.5.9] Se realiza un análisis previo basado en el conocimiento exhaustivo del sistema
- [H.VM.5.b] Se realizan pruebas para determinar explotabilidad de vulnerabilidades identificadas
- [L.7.2.6] Se dispone de un sistema de evacuación de humos
- [AUX.wires.a] Se controlan todos los accesos al cableado
- [AUX.wires.b] Hay protección prevista contra daños o interceptaciones no autorizadas (conductos blindados, cajas o salas cerradas, ...)
- [H.IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello
- [HW.op.3.8] Se dispone de una póliza de seguro para los equipos fuera de su lugar de trabajo
- [COM.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados
- [H.IR.2.a] Actuación frente a fallos del software
- [H.tools.VA.2] Se actualiza regularmente el conjunto de vulnerabilidades utilizado por el proveedor
- [H.tools.VA.3] Se revisa el sistema operativo
- [MP.cont.7] Se migra la información de un soporte a otro en función de su vida útil
- [L.design.7] Hay una separación entre áreas de seguridad y de acceso público
- [K.comms.9] Las claves se destruyen de forma segura
- [L.AC.3.2] Se comprueba la identidad de las visitas
- [L.AC.c.5] Las llaves se cambian cuando se hayan comprometido o exista sospecha de ello
- [L.AC.c.6] Las combinaciones se cambian o modifican cuando han sido comprometidas o exista sospecha de ello
- [H.ST.2.3] Autorización de datos
- [H.AC.7.a] Los privilegios se anulan cuando termina la autorización
- [H.AU.3.6] No se incluye en los registros información sensible
- [HW.PCD.8.6] Se han establecido los requisitos sobre copias de seguridad (backups)
- [H.IR.d.5] Se comprueba la integridad de los sistemas y de las medidas de control de seguridad
- [K.comms.5] Las claves se generan en un entorno separado del de explotación
- [COM.SC.3] Se eliminan, o modifican, las cuentas estándar de administrador

- [COM.SC.4] Sólo los administradores autorizados pueden modificar la configuración
- [COM.SC.5] Los servicios activados se configuran de forma segura
- [L.7.8.1] Se ha contratado una póliza de continente (edificios)
- [H.IR.2.2] Actuación frente a ataques de denegación de servicio (DoS)
- [SW.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados
- [HW.CM.6] Se priorizan las actuaciones encaminadas a corregir riesgos elevados
- [L.7.4.3] Se selecciona el emplazamiento para minimizar el riesgo de accidentes naturales o industriales
- [IP.BS.2.6] Se aplica la regla de 'seguridad por defecto'
- [E.1.c] Se garantiza la disponibilidad de la información
- [E.1.d] Se establecen controles para asegurar la recuperación de información cuando se requiera
- [H.IR.2.3] Actuación ante fallos del sistema e interrupciones del servicio
- [SW.SC.2] Se eliminan, o modifican, las cuentas estándar de usuario
- [H.AC.a.2] Tras un intento fallido existe un retardo hasta que el siguiente intento sea posible
- [H.AC.a.5] Se limita el tiempo permitido para efectuar el proceso de conexión
- [COM.wifi.a] Se autentican los dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)
- [H.ST.1] Todos los procesos críticos requieren al menos 2 personas
- [H.ST.2.5] Administrador de comunicaciones (redes)
- [L.7.8.2] Se ha contratado una póliza de contenido
- [SW.op.8.1] Se asegura la integridad
- [G.exam.4.2] Se reparan con diligencia los defectos descubiertos que implican un cierto riesgo
- [H.tools.VA.4] Se revisan las aplicaciones base del sistema
- [L.AC.4.5] El diseño es difícil de falsificar
- [L.AC.4.8] Los pases no contienen datos que permitan, en caso de pérdida, obtener información acerca de su finalidad (simplemente contiene una dirección para su envío)
- [L.7.2.2] Las áreas están compartimentadas (por sectores)
- [L.7.2.3] Existen vías de evacuación
- [L.7.2.5] Se dispone de un sistema de iluminación de emergencia
- [L.7.2.a] Se dispone de un plan de autoprotección
- [L.7.3.2] Se dispone de llaves de paso que permiten el corte del suministro de agua
- [H.AU.3.4.1] Los registros se protegen contra accesos de lectura no autorizados
- [H.AU.3.4.2] Los registros se protegen contra borrado y modificación no autorizados
- [H.AU.3.4.5] Se cumplen los requisitos de continuidad de negocio
- [MP.cont.4] Se duplican los soportes críticos

- [K.comms.7.1] Contenedor seguro
- [S.SC.1] Se eliminan, o modifican, las cuentas estándar de usuario
- [HW.PCD.a.2] Se dispone de mecanismos para reacción urgente a incidentes
- [L.design.9] Se encuentran separadas las áreas gestionadas por otros
- [H.AC.c.2] Bloqueo de la pantalla al dejar desatendido el equipo
- [H.AC.c.3] Cancelación o bloqueo de sesiones al dejar desatendido el equipo
- [H.AC.c.4] Los equipos se desconectan y se apagan al finalizar las actividades
- [H.AC.d.1] Tras un periodo establecido de inactividad, se activa el protector de pantalla con contraseña
- [H.AC.d.2] Tras un periodo determinado de inactividad, se terminan automáticamente las sesiones establecidas (en sesiones que soporten un riesgo elevado)
- [H.AC.d.3] Tras un periodo determinado de inactividad, se terminan automáticamente las sesiones establecidas en acceso remoto
- [H.AC.5.3] Se restringe el uso de las aplicaciones a ciertas estaciones
- [H.AC.b.2] Se definen ventanas horarias para determinados procesos
- [H.AC.b.3] Se restringe el acceso a los sistemas a los periodos horarios específicos de trabajo
- [H.AC.b.4] Se solicita re-autenticación para ciertas actuaciones clasificadas como críticas
- [D.backup.2.3.2] Se hacen copias de las claves para descifrar
- [D.backup.2.3.3] Se hacen copias de la información de verificación de firmas
- [D.backup.2.3.5] Periódicamente, se verifican las copias de seguridad
- [L.7.1] La iluminación de emergencia cubre todas las áreas necesarias para garantizar la continuidad de las misiones críticas
- [SW.op.c.2] Se asegura la integridad
- [IP.2.1] Se identifican y autentican los usuarios antes de establecer el enlace
- [IP.2.2] Se identifican y autentican los procesos usuarios antes de establecer el enlace
- [IP.2.3] El servidor se identifica y autentica antes de establecer el enlace
- [BC.DRP.5.6] Están previstos los medios alternativos de almacenamiento de la información
- [BC.DRP.5.7] Están previstos los medios alternativos de procesamiento de la información
- [BC.DRP.5.8] Están previstos medios alternativos de comunicación
- [MP.IC.4] Se garantiza la integridad del contenido
- [MP.IC.5] Se firma el contenido

- [AUX.power.6.4.2] Sistema de alimentación redundante que garantiza el funcionamiento de los equipos críticos, y la continuidad de las operaciones
- [HW.op.2.1.2] para evitar accesos no autorizados
- [L.6.3.3] La alimentación es redundante
- [COM.C.3.1] Dispositivo lógico
- [H.IR.2.b] Actuación frente a estaciones base wifi no auorizadas
- [L.design.d] Las instalaciones son discretas minimizando indicaciones sobre su propósito
- [SW.op.9.2] Se asegura la integridad
- [H.ST.2.1] Usuario del sistema
- [H.ST.2.2] Entrada de datos
- [H.ST.2.4] Administrador del sistema
- [H.ST.2.6] Administrador de Seguridad
- [H.ST.2.7] Desarrollo y mantenimiento de sistemas
- [H.AC.9.1.3] Los accesos se controlan según lo autorizado por el propietario del recurso
- [COM.start.5] Se verifica el funcionamiento de los registros de actividad
- [H.tools.VA.1] La herramienta se actualiza regularmente
- [H.tools.VA.5] Se revisan las aplicaciones específicas de la organización
- [L.AC.4.4] Se usan diferentes tipos de pases según la categoría del personal (personal propio, visitas, etc.)
- [L.AC.4.6] Los pases incluyen una fotografía de la persona identificada
- [L.AC.4.7] Los pases permiten reconocer visualmente el tipo de áreas a las que puede acceder su portador
- [SW.SC.3] Se eliminan, o modifican, las cuentas estándar de administrador
- [SW.SC.4] Sólo los administradores autorizados pueden modificar la configuración
- [SW.SC.5] Las funciones activadas se configuran de forma segura
- [H.tools.AV.2] La base de datos de virus se actualiza regularmente
- [H.VM.7.1] Se reparan urgentemente las vulnerabilidades que implican un alto riesgo
- [S.3.5.3.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello
- [COM.wifi.4] Se eliminan las claves por defecto en tarjetas y puntos de accesos antes de su despliegue
- [COM.wifi.6] Se deshabilitan los protocolos de gestión no esenciales
- [H.AU.3.7] Los registros evitan información que pueda ser útil a un atacante
- [L.design.2] El número de entradas se reduce al mínimo necesario
- [L.AC.c.2] Las áreas de seguridad disponen de algún tipo de llave, combinación o dispositivo de seguridad para acceder a las mismas
- [L.AC.3.1] Se requiere autorización previa para el acceso de visitas, personal de mantenimiento, o personal de empresas contratistas

- [H.ST.3.7] Los desarrolladores no pueden pasar aplicaciones a producción
- [H.ST.3.8] Los desarrolladores no pueden configurar aplicaciones en producción
- [PS.5.1.1] Personal propio: se comprueba previamente que el personal cumple los requisitos del puesto
- [MP.cont.1] Se toman medidas contra el deterioro físico del soporte
- [MP.cont.5] Las copias de los soportes críticos se almacenan en un lugar alternativo
- [L.AC.a] Se evita el trabajo no supervisado
- [L.2.5] Las áreas no se identifican en directorios telefónicos y vestíbulos
- [L.AC.7] Se evita que el acceso físico para operación y mantenimiento abra el acceso a otros activos
- [MP.5.5] El soporte se protege técnicamente antes de su salida
- [HW.op.2.3] Se controla el acceso a los equipos de presentación (impresoras, pantallas, etc.)
- [COM.SC.1] Se reducen las opciones a las mínimas necesarias
- [SW.op.c.3] Se asegura la autenticidad
- [H.IR.7.4] Se mantienen contactos con los operadores de telecomunicaciones
- [MP.4.1.3] Se reduce al mínimo imprescindible la distribución de soportes
- [HW.op.2.5] Los elementos fáciles de llevar se encadenan
- [HW.op.2.6] El equipamiento se protege convenientemente cuando no se emplea
- [PS.5.1.2] Personal subcontratado: se comprueba previamente que el personal cumple los requisitos del puesto
- [H.AC.a.1] Se restringen usuarios y grupos de usuarios a ciertas estaciones
- [H.tools.AV.4] Se revisa cada aplicación cuando arranca
- [H.tools.AV.6] Se revisa el contenido de las páginas web que se visitan
- [H.tools.AV.8] Se revisan los ficheros recibidos en un medio removible
- [D.3.2.1] Se eliminan notas y comentarios
- [D.3.2.2] Se elimina la información de versiones previas
- [D.3.2.3] Se eliminan meta-datos
- [S.1.2.7.1.1] Su confidencialidad
- [S.1.2.7.1.2] Su integridad
- [S.1.2.7.1.3] Su autenticidad
- [S.1.2.7.2.1] Su confidencialidad
- [S.1.2.7.2.2] Su integridad
- [S.1.2.7.2.3] Su autenticidad
- [S.1.2.a.3] Se comprueba la publicación de actualizaciones por parte del proveedor
- [S.1.2.a.4] El SW se actualiza regularmente (parches, versiones, etc.)

- [COM.wifi.9] Se desactiva el modo de conexión ad-hoc en los dispositivos de usuario
- [L.6.1] El perímetro está claramente definido con una valla, muro o similar
- [HW.op.2.7] Los dispositivos móviles o portátiles se almacenan en contenedores de seguridad
- [S.SC.2] Se eliminan, o modifican, las cuentas estándar de administrador
- [MP.clean.5.1.1] Sobreescritura
- [COM.cont.7] Se realizan copias de seguridad de la configuración (backup)
- [COM.aut.5] Canal de autenticación
- [COM.CM.c] Se prueba previamente en un entorno que no esté en producción
- [SW.op.c.4] En cuanto es posible, se limpian los almacenes temporales
- [SW.op.3.1] Se chequea regularmente que el ejecutable no se ha modificado
- [HW.op.2.1.1] para evitar accesos innecesarios
- [H.AC.6.2] La BIOS está protegida con contraseña
- [H.AC.6.3] Se restringe el acceso a ciertas estaciones
- [SW.op.8.3] Se asegura la autenticidad
- [S.start.4] Se verifica el funcionamiento de los registros de actividad
- [L.AC.2.8] Los admitidos están acompañados permanentemente (escoltas) según política
- [L.6.3.1] El sistema de detección de intrusión está centralizado
- [L.6.3.5] Se dispone de protección anti sabotage
- [L.6.3.7] Periódicamente se revisa y se realizan las actividades de mantenimiento
- [H.IR.2.d] Detección y reacción frente a actividades de robo de datos de carácter personal
- [H.VM.5.3] Se prueba desde Internet (atacantes externos)
- [H.VM.5.7] Se realizan pruebas a nivel de aplicaciones
- [H.VM.5.a] Se identifican las vulnerabilidades potenciales a partir del análisis previo
- [H.VM.5.c] Las pruebas se repiten regularmente
- [S.1.2.8] Medidas frente a la recepción de spam
- [COM.cont.a.1] Se dispone de conexión redundante (mediante doble tarjeta de red) de los dispositivos críticos
- [SW.op.7.2] Se asegura la integridad
- [SW.SC.1] Se reducen las opciones a las mínimas necesarias
- [L.6.2.1] Se dispone de una barrera de alta seguridad: alta resistencia a la escalada y apertura de brechas
- [SW.op.7.3] Se asegura la autenticidad
- [HW.op.3.5] El activo se protege técnicamente antes de su salida
- [HW.op.3.6] Se proporciona una seguridad equivalente a la de los equipos instalados dentro para el mismo propósito

- [H.VM.7.2] Se reparan con diligencia las vulnerabilidades que implican un cierto riesgo
- [G.exam.4.1] Se reparan urgentemente los defectos descubiertos que implican un alto riesgo
- [S.3.7.4] Destrucción de la información en el proveedor
- [SW.op.4] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico
- [H.AC.7.9] El sistema mantiene los privilegios asociados a cada usuario
- [H.AU.2.1.1] Se guardan separadas de los sistemas de desarrollo y operación
- [D.DS.4.1] Se garantiza la disponibilidad de los certificados correspondientes para cuando haya que validar la firma
- [D.DS.4.2] Se garantiza la disponibilidad de los datos de verificación y validación correspondientes para cuando haya que validar la firma
- [S.CM.4] Se hace un seguimiento permanente (servicios externos)
- [HW.cont.8] Se hacen copias de seguridad de las claves de descifrado
- [HW.PCD.8.7] Se instala software antivirus y se mantiene actualizado
- [COM.start.4] Se verifica el funcionamiento de los controles de seguridad
- [COM.op.1.4.1] Está prohibido el diagnóstico remoto
- [MP.clean.3] Se realiza una limpieza segura del contenido de todo soporte reutilizable del que se desprenda la organización
- [MP.clean.4] Se retiran todas las etiquetas y marcas
- [L.AC.2.4] La autorización para acceder se verifica antes de conceder el acceso
- [L.AC.2.d] Los procedimientos de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones
- [L.AC.c.8] Las combinaciones se cambian o modifican al menos cada seis meses
- [H.ST.3.3] Se impide que alguien pueda autorizarse a sí mismo
- [BC.4.1] Se adoptan medidas preventivas
- [SW.op.9.3] Se asegura la autenticidad
- [COM.DS.1.2] Se controla el acceso de los usuarios al segmento
- [COM.DS.1.3] Se controla la salida de información del segmento
- [COM.DS.2] Los usuarios se segregan en dominios
- [L.AC.2.b.2] Se dispone de un mecanismo anti pass-back
- [L.AC.2.b.3] La alimentación de potencia es redundante
- [COM.SC.2] Se eliminan, o modifican, las cuentas estándar de usuario
- [AUX.wires.1] La gestión está centralizada
- [AUX.wires.2] Se utiliza una herramienta de gestión
- [AUX.wires.6] Se realiza un mantenimiento regular del cableado
- [L.AC.4.3] Es obligatorio empleo de un pase (ej. tarjeta) en el interior del recinto
- [HW.op.2.1.3] para evitar daños (incendios, agua, ...)

- [MP.end.6.1.1] Desintegración: trocear en componentes separados
- [H.IA.5.2] Hay cuentas específicas para administradores de seguridad
- [H.AC.7.b] Los privilegios se revisan cuando el usuario cambia de responsabilidades o de función
- [H.AC.7.c] Los privilegios se anulan cuando el usuario abandona la organización
- [L.AC.5] Los accesos permanecen cerrados fuera de las horas de trabajo
- [SW.op.c.1] Se asegura la confidencialidad
- [AUX.power.6.4.1] Sistema de alimentación ininterrumpida (SAI) que permite el funcionamiento de los equipos críticos, hasta su correcto cierre y apagado
- [H.IR.6] Ayuda a los afectados
- [H.IR.7.1] Se mantienen contactos con las autoridades
- [H.IR.7.2] Se mantienen contactos con los organismos reguladores
- [H.IR.7.3] Se mantienen contactos con los proveedores de servicios de información
- [H.IR.7.5] Se participa en foros de seguridad
- [L.design.8.1] Se dispone de áreas específicas para equipos informáticos
- [L.design.8.2] Se dispone de áreas donde se presenta información (pantallas, impresoras, ...)
- [L.design.8.3] Se dispone de áreas con acceso a medios de transmisión
- [L.design.8.4] Se dispone de áreas para elementos auxiliares
- [D.backup.1.1] Las copias de seguridad se protegen de acuerdo a la información que contienen
- [L.7.2.d.1] Se dispone de medios manuales de extinción de incendios (extintores portátiles, hidrantes, BIE's, etc.)
- [SW.4.4] Se controla el número máximo de usuarios permitidos
- [SW.4.5] Se controla la instalación de software autorizado y productos con licencia
- [SW.op.a.1.1] Se requiere autorización previa
- [SW.op.a.2.3] Se verifica la integridad del código
- [SW.op.a.2.4] Se analiza por si contuviera código malicioso
- [HW.start.5] Se verifica el funcionamiento de los controles de seguridad
- [COM.aut.2] Se verifica la identidad del usuario antes de entregarle el mecanismo de autenticación
- [COM.aut.3] Se autentica el origen de la conexión
- [COM.aut.6] Se toman medidas para impedir el secuestro de sesiones establecidas
- [COM.CM.3] Se hace un seguimiento permanente de actualizaciones
- [COM.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
- [COM.CM.b] Se retienen copias de las versiones anteriores de configuración

- [MP.4.3.3.1] Se recurre a transportes y mensajeros identificados y autorizados
- [MP.4.3.5] Se utilizan contenedores adecuados contra cualquier daño físico y de acuerdo a las especificaciones de los fabricantes
- [AUX.wires.9] Se evitan rutas a través de áreas públicas
- [SW.SC.6] Se aplica la regla de 'seguridad por defecto'
- [L.AC.2.b.1.1] Basado en clave (PIN) o tarjeta
- [L.6.3.4.1] Supervisado por personal de seguridad durante las horas de trabajo
- [H.AC.4.3] No se puede acceder a la información sin una verificación previa de los derechos de acceso
- [H.AC.a.3] Se bloquea la cuenta tras un número limitado de intentos fallidos
- [H.AC.a.4] Se requiere autorización para restablecer una cuenta bloqueada
- [H.AC.a.g] Las contraseñas no pueden ser almacenadas en ningún proceso automático (macros, teclas de función, etc.)
- [H.tools.AV.5] Se revisan los anexos al correo electrónico
- [COM.cont.1] Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)
- [MP.IC.8.1] Mecanismo basado en MAC (Código de Autenticación de Mensaje)
- [L.6.3.2] El instalador es una empresa autorizada
- [IP.BS.2.2] Se eliminan, o modifican, las cuentas estándar de usuario
- [IP.BS.2.3] Se eliminan, o modifican, las cuentas estándar de administrador
- [IP.BS.2.4] Sólo los administradores autorizados pueden modificar la configuración
- [IP.BS.2.5] Los servicios activados se configuran de forma segura
- [MP.cont.6] Se establece la frecuencia con que se realizarán copias de seguridad (backup)
- [K.comms.6.1] Aplicación informática
- [MP.4.3.6.1] Entrega en mano
- [MP.4.3.6.2] Uso de contenedores cerrados
- [MP.4.3.6.5] Cifrado de la información
- [H.AU.3.4.3] Se hacen copias de seguridad
- [H.AU.3.4.4] Las copias de seguridad garantizan la misma seguridad
- [H.AU.3.4.6] En caso de fallo del sistema, se garantiza la disponibilidad de los datos registrados hasta ese momento
- [AUX.6] Se disponen medidas frente a posibles robos
- [D.backup.2.4.1.2.1] Papel
- [D.DS.6.1] Dispositivo lógico
- [H.VM.7.3] Se planifica la reparación de las vulnerabilidades que implican un riesgo bajo
- [HW.cont.9.1] Equipo alternativo
- [COM.op.2.1.1] Se monitorizan excepciones e incidentes de seguridad
- [COM.op.2.1.2] Seguimiento y corrección de los incidentes y errores

- [COM.aut.4.2.2.2] Los certificados tienen una validez limitada y se renuevan periódicamente
- [S.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
- [SW.op.5.3] Las aplicaciones críticas se instalan en máquinas dedicadas
- [SW.op.8.4] Se asegura la confidencialidad
- [SW.CM.a] Control de versiones de toda actualización del software
- [SW.CM.d] Se retienen copias de las versiones anteriores de configuración
- [SW.CM.i] Se actualizan todos los procedimientos de producción afectados
- [HW.CM.9] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
- [HW.CM.i] Se actualizan todos los procedimientos de producción afectados
- [HW.PCD.5.4] Los dispositivos portátiles se guardan en lugar seguro cuando no están en uso
- [IP.SPP.6.1] Se asegura la autenticidad del origen
- [IP.SPP.6.2] Se asegura la integridad de la información
- [IP.SPP.6.3] Se asegura la confidencialidad de la información
- [MP.end.4] Se controla el acceso a los soportes que van a ser eliminados
- [NEW.SW.5.1.1.1] Mecanismo(s) de control de acceso
- [NEW.SW.5.1.1.2] Mecanismo(s) de identificación y autenticación
- [NEW.SW.5.1.1.3] Mecanismo(s) de registro y auditoría
- [NEW.SW.5.1.1.4] Soporte de la confidencialidad requerida
- [NEW.SW.5.1.1.5] Soporte de la integridad requerida
- [NEW.SW.5.1.1.6] Soporte de la disponibilidad requerida
- [L.design.b] Se encuentran separados los accesos para personas y vehículos
- [K.comms.4.1] Las claves se cambian regularmente
- [K.comms.4.4] Se destruyen las claves retiradas del servicio
- [H.AC.5.2] Las utilidades del sistema están separadas de los aplicativos
- [H.AC.5.4] Se restringe el acceso a un número limitado de usuarios
- [H.AC.b.1] Se dispone de mecanismos para limitar el periodo de tiempo en que se puede establecer cada tipo de conexión
- [COM.I.1] Mecanismo basado en MAC (Código de Autenticación de Mensaje)
- [L.cont.3] Se dispone de instalaciones alternativas
- [AUX.wires.g] El cableado es tolerante a fallos (redundancia de líneas críticas, etc.)
- [L.design.5] Se dispone de protección en los conductos y aberturas (falso techo, conductos de aire, etc.)
- [L.AC.9] Se exige que los puestos de trabajo están despejados
- [MP.4.1.2] Los soportes se guardan en lugar seguro cuando no están en uso

- [H.IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)
- [H.IA.4.2.5.1] Las cuentas que ya no son necesarias se eliminan o se bloquean
- [PS.5.3.2] Recuperación de los elementos de seguridad a devolver (llaves, tarjetas, etc.)
- [BC.DRP.5.4] Están previstas instalaciones alternativas
- [BC.DRP.5.5] Las copias de seguridad (backup) se realizan con la frecuencia acordada
- [HW.cont.1] Se dimensiona holgadamente y se planifica la adquisición de repuestos
- [IP.BS.2.1] Se reducen las opciones a las mínimas necesarias
- [S.start.3] Se verifica el funcionamiento de los controles de seguridad
- [S.3.5.4] Se toman medidas para impedir el secuestro de sesiones establecidas
- [SW.op.7.1] Se asegura la confidencialidad
- [IP.BS.3.1] Se verifica la actualidad de sus componentes (parches software)
- [IP.BS.3.2] Se verifica su configuración de seguridad
- [NEW.SW.5.4.4] Se controla el acceso a las herramientas de desarrollo
- [NEW.SW.5.5.5] Se verifica el funcionamiento de los controles de seguridad
- [NEW.SW.5.5.6] Se verifica que el nuevo sistema no afecta negativamente a las otras funciones del sistema en el que va a operar
- [COM.C.4.1] ~ 64 bits
- [H.IR.2.6] Actuación frente a alarmas de los sistemas de detección de intrusión
- [H.IR.2.7] Actuación frente a alarmas de los sistemas de prevención de intrusión
- [H.IR.2.9] Actuación frente a alarmas de uso no autorizado del sistema
- [H.IR.2.e] Actuación frente a otros incidentes
- [AUX.wires.d] Se protegen los cuadros de distribución
- [COM.DS.3.1] Separación mediante redes conmutadas (router / switch)
- [SW.op.9.4] Se asegura la confidencialidad
- [HW.op.3.2] Se identifica a las personas autorizadas
- [NEW.SW.5.3.8] Se mentiene un archivo de versiones anteriores
- [D.backup.2.3.4] Las copias de seguridad, y los procedimientos, se almacenan en lugares diferentes de tal forma que los datos originales y las copias no se vean afectados simultáneamente por un incidente
- [H.IA.5.1] Hay cuentas específicas para administradores del sistema
- [COM.start.6] Se requiere haber pasado las pruebas de aceptación
- [AUX.power.3] Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas

- [L.AC.c.4] Se custodian de forma segura, incluidos los duplicados
- [H.IR.g] Se toman medidas para prevenir la repetición
- [H.ST.3.a] Los usuarios ni desarrollan ni pueden modificar los desarrollos
- [H.ST.3.b] Los usuarios ni configuran ni pueden modificar la configuración
- [AUX.AC.3] Control de temperatura
- [AUX.AC.4] Control de humedad
- [D.DS.7.1] RSA-1024 (o equiv.) + hash 160 bits
- [IP.BS.4.4] Se realizan copias de seguridad periódicas de la configuración
- [SW.op.2] Los sistemas de producción no contienen herramientas de desarrollo
- [COM.op.1.3.1.2.1] Por tipo
- [COM.op.1.3.1.2.2] Por sentido del flujo
- [IP.SPP.4.1] Se garantiza que todo el tráfico pasa por el sistema de defensa perimetral
- [IP.SPP.4.2] Se bloquea todo el tráfico, excepto el explícitamente aprobado
- [HW.op.2.4] Se controla el acceso a los dispositivos móviles y portátiles
- [S.3.7.5] Desactivación del servicio por personal autorizado
- [MP.4.1.1] Se imponen restricciones de acceso para impedir el acceso no autorizado
- [SW.backup.4] Las copias de seguridad se protegen de acuerdo al SW que contienen
- [COM.aut.4.2.1] Se protege el uso por medio de contraseña
- [COM.op.1.3.1.2.3] Por períodos de tiempo
- [S.3.6.3] Se dispone de medios alternativos
- [K.comms.4.5] Los certificados de firma se revocan cuando dejan de ser válidos
- [H.AC.4.4] Se establecen menús específicos para controlar los accesos a las funciones de las aplicaciones
- [H.AC.4.5] Se controlan los privilegios de los usuarios (lectura, escritura, modificación, borrado, ejecución)
- [H.AC.4.6] Se controlan los privilegios de otras aplicaciones
- [H.tools.AV.1] El programa se actualiza regularmente
- [H.tools.AV.3] Se revisan los programas y servicios de arranque del sistema
- [H.tools.AV.7] Se revisan todos los ficheros descargados
- [H.tools.AV.9] Se revisan medios removibles cuando se conectan al sistema de información
- [S.1.2.9.1] anti-virus
- [S.1.2.9.2] anti-spyware
- [S.1.2.9.3] código activo
- [S.1.2.9.4] datos adjuntos
- [S.1.2.9.5] Se deshabilita la apertura automática de datos adjuntos
- [S.1.2.a.2] Se configuran de forma segura los protocolos autorizados

- [COM.wifi.5] Se desactivan los puertos y servicios no usados
- [COM.wifi.7] Se aplican restricciones al protocolo SNMP en redes wireless
- [COM.wifi.b] Se controlan las direcciones IP
- [COM.op.3] Se prevé protección frente a análisis del tráfico
- [L.design.a] Se encuentran separadas las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.)
- [L.7.2.h] Se garantizan las condiciones adecuadas de aproximación para las fuerzas de ayuda exterior
- [L.7.3.1] Se ha diseñado la instalación garantizando que no hay canalizaciones cercanas de agua
- [H.IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador
- [SW.start.7] Se requiere haber pasado las pruebas de aceptación
- [HW.start.6] Se requiere haber pasado las pruebas de aceptación
- [COM.cont.8] Se hacen copias de seguridad de las claves de autenticación
- [COM.cont.9] Se hacen copias de seguridad de las claves de descifrado
- [COM.CM.a] Realización por personal debidamente autorizado
- [S.cont.1.1] Se han dimensionado los dispositivos accesibles (cortafuegos, servidores, ...) para soportar la máxima carga prevista
- [S.2.9.4] Implantación de mecanismos de autenticación de las partes
- [S.3.5.1] Se autentica el servidor antes de transferir información alguna
- [SW.backup.6] Las copias de seguridad se almacenan en lugares alternativos
- [SW.op.7.4] Se realizan copias de seguridad (backup)
- [NEW.SW.5.6.1] Las pruebas no usan datos reales
- [AUX.wires.f] Se emplean recubrimientos que no son inflamables ni tóxicos
- [NEW.SW.5.3.1] Se controla el acceso al código fuente
- [COM.cont.3] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes
- [AUX.cont.1] Se siguen las recomendaciones del fabricante o proveedor
- [H.IA.5.3] Hay cuentas específicas para actividades de auditoría
- [H.AC.7.2] En la asignación de privilegios se tiene en cuenta el principio de 'privilegio mínimo necesario para realizar las tareas asignadas'
- [H.AC.7.3] En la asignación de privilegios se tiene en cuenta el principio de 'necesidad de conocer'
- [D.TS.4.1] Se garantiza la disponibilidad de los certificados correspondientes para cuando haya que validar el fechado
- [D.TS.4.2] Se garantiza la disponibilidad de los datos de verificación y validación correspondientes para cuando haya que validar el fechado

- [S.CM.a] Se realiza por personal debidamente autorizado
- [SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches
- [SW.CM.b] Realización por personal debidamente autorizado
- [SW.CM.e] Se prueba previamente en un equipo que no esté en producción
- [HW.7.1] El equipo se instala atendiendo a las especificaciones del fabricante
- [HW.7.2] Se evita que por acceder a este equipo se abra el acceso a otros
- [HW.7.3] Se evita el acceso visual a pantallas y monitores por personas no autorizadas
- [HW.CM.b] Realización por personal debidamente autorizado
- [HW.CM.d] Se prueba previamente en un entorno que no esté en producción
- [COM.op.1.3.1.1] Restricciones basadas en requisitos de negocio
- [COM.op.1.6.1] Basado en los flujos de información permitidos
- [COM.op.1.6.2] Comprobación de direcciones de origen y destino
- [COM.op.1.6.3.1] Líneas o números de teléfono dedicados
- [COM.op.1.6.3.2] Conexión automática de puertos a sistemas de aplicaciones específicas o a pasarelas (gateways) de seguridad
- [COM.op.1.6.3.3] Limitación de opciones de menú para usuarios
- [COM.op.1.6.3.4] Se evitan los recorridos cíclicos ilimitados en la red
- [COM.op.1.6.3.5] Forzar el uso por usuarios de redes externas de ciertos sistemas de información específicos y / o pasarelas (gateways) de seguridad
- [COM.op.1.6.3.6] Se emplean pasarelas de seguridad para controlar activamente las comunicaciones permitidas
- [COM.op.1.6.3.7] Restricción de acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para ciertos grupos de usuarios dentro de la Organización
- [IP.5.1.1] Todo el tráfico atraviesa el filtro
- [AUX.power.4] Interruptor general de la alimentación del sistema situado en la entrada de cada área
- [AUX.power.5] Interruptores etiquetados y protegidos frente a activaciones accidentales
- [L.design.1] El diseño atiende a las reglas y normas relevantes sobre salud y sanidad
- [L.design.4.1] Las ventanas de fácil acceso visual tienen cristales opacos
- [L.design.4.2.2] tienen barrotes o rejas
- [L.AC.1] El acceso tiene que ser a través de un área de recepción
- [L.AC.6] Las áreas de trabajo se cierran y controlan periódicamente cuando están vacías
- [L.AC.8] Las salidas de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones
- [L.AC.c.3] Solamente el personal autorizado puede usarlos

- [L.AC.c.7] Las combinaciones se cambian o modifican cuando haya cambios de personal que haya tenido acceso a las mismas
- [H.ST.3.6] Se designa personal específico para la realización de transferencias de fondos
- [SW.op.9.1] Se realizan copias de seguridad (backup)
- [AUX.wires.8.1] Cableado de alimentación
- [AUX.wires.8.2] Cableado de datos
- [AUX.wires.e] Se protejen antenas y repetidores
- [L.2.6] El personal sólo conoce la existencia de estas áreas, o de sus actividades, si lo necesita para su trabajo
- [IP.BS.4.2] Se exige autenticación del operador para cambios de configuración
- [MP.cont.2] Se realiza el mantenimiento periódico según especificaciones de los fabricantes
- [MP.cont.3] Los soportes se almacenan de acuerdo a las especificaciones del fabricante
- [HW.cont.3] El mantenimiento lo realiza personal debidamente autorizado
- [HW.cont.7] Se hacen copias de seguridad de la configuración
- [MP.IC.9.1.1.1] ~ 64 bits
- [D.backup.2.3.1] Se hacen copias de la información en consonancia con sus requisitos de disponibilidad
- [D.backup.2.3.6] Periódicamente, se prueban los procedimientos de restauración
- [SW.op.8.2] Se realizan copias de seguridad (backup)
- [MP.cont.8] Se hacen copias de seguridad de las claves de descifrado
- [HW.cont.2] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes
- [S.start.5] Se requiere haber pasado las pruebas de aceptación
- [S.start.9] Paso a producción
- [HW.op.4.2] Todos los terminales conectados están unívocamente identificados (direcciones MAC, IPs estáticas, etc.)
- [HW.op.4.3] Los usuarios no pueden alterar la identificación del equipo
- [HW.op.4.4] Los dispositivos de identifican y autentican antes de conectarse al sistema
- [NEW.SW.5.4.1.1] Separación lógica
- [NEW.SW.5.5.1.1] Separación lógica
- [H.IA.3.3] Las cuentas de invitados están sometidas a un control estricto
- [H.IA.4.4] Se limita el número de autenticadores necesarios por usuario
- [H.IA.4.5] Los autenticadores se distribuyen de forma segura
- [SW.op.a.2.2] Se verifica el origen del código
- [SW.op.b.1] Se imponen restricciones en el uso de programas propios
- [SW.op.b.2] Se imponen restricciones en el uso de código externo

- [COM.cont.2] Se dimensiona holgadamente y se planifica la adquisición de repuestos
- [COM.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'
- [COM.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'
- [COM.wifi.2] Al instalar un punto de acceso (AP) se tiene en cuenta el alcance de la señal para evitar una exposición gratuíta a ataques
- [IP.4.1.1] Todo el tráfico atraviesa el filtro
- [IP.BS.1.1] Se instalan las nuevas versiones del fabricante del producto
- [IP.BS.1.2] Se instalan los parches del fabricante del producto
- [IP.BS.1.4] Se exige autenticación del operador para cambios del programa
- [L.design.3.1] Se dispone de puertas de acceso reforzadas
- [L.design.4.2.1] tienen cristales blindados
- [D.C.4.1.1.1] ~ 64 bits
- [S.3.5.3.1.1] por programa (SW)
- [AUX.AC.5] Control de flujo de aire
- [S.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'
- [S.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'
- [S.3.5.2.1.1] Se protege el secreto en el cliente
- [S.3.5.2.1.2] Robusto frente a ataques de fuerza bruta
- [S.3.5.2.1.3] Se protege el canal de autenticación
- [SW.op.d] Regularmente se realiza un análisis de vulnerabilidades, y se actúa en consecuencia
- [SW.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'
- [SW.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'
- [HW.op.2.2] Los elementos que requieren especial protección se aislan para reducir el nivel general de protección requerido
- [HW.CM.3] Se siguen las recomendaciones del fabricante o proveedor
- [HW.CM.4] Se hace un seguimiento permanente de actualizaciones
- [HW.CM.7] Se mantiene en todo momento la regla de 'funcionalidad mínima'
- [HW.CM.8] Se mantiene en todo momento la regla de 'seguridad por defecto'
- [HW.CM.c] Se retienen copias de las versiones anteriores de configuración
- [COM.op.1.3.1.2.4] Por origen / destino
- [IP.SPP.2] Se valida el formato de todos los datos en tránsito
- [IP.SPP.3.2] El tráfico se identifica antes de autorizar su paso
- [IP.SPP.5.1] Identificación y autenticación de los usuarios
- [IP.SPP.5.2] Identificación y autenticación de los nodos

- [IP.SPP.5.3] Autorización de acceso
- [IP.SPP.5.4] Listas blancas (white lists)
- [IP.SPP.5.5] Listas negras (black lists)
- [IP.SPP.5.6] Etiquetas de seguridad de los objetos intercambiados
- [IP.SPP.5.7] Información de control de red (nivel 3)
- [IP.SPP.5.8] Información de control de aplicación (nivel 7)
- [MP.5.2] Se identifica a las personas autorizadas
- [NEW.SW.5.1.2] Se tratan específicamente los datos de prueba
- [BC.DRP.7.2] Se simulan situaciones de crisis
- [BC.DRP.7.3] Se realizan pruebas de recuperación técnica
- [BC.DRP.7.4] Se realizan pruebas de recuperación en un centro alternativo
- [BC.DRP.7.5] Se realizan pruebas de los recursos y servicios de los proveedores
- [BC.DRP.7.6] Se registran las lecciones aprendidas y se aplican dentro del proceso de mejora continua
- [SW.backup.2] Se hacen copias de las aplicaciones críticas para el negocio
- [SW.backup.3] Se hacen copias de los sistemas operativos en explotación
- [SW.backup.5] Regularmente se verifica que las copias pueden ser restauradas correctamente
- [S.cont.1.2] Se ha dimensionado adecuadamente la capacidad de almacenamiento de los dispositivos de registro (logs) de actividad
- [S.cont.1.3] Los recursos se priorizan en base a la prioridad del servicio afectado
- [S.start.1] Puesta en pre-producción
- [S.2.9.3] Controles sobre el desarrollo del proceso (fijación de precios, contratación, etc.)
- [S.2.9.5] Establecimiento de mecanismos de autorización del proceso
- [NEW.SW.5.5.3] Se emplean cuentas de usuario diferentes: pruebas y producción
- [HW.cont.a.1] Equipo de alta disponibilidad con sistema de almacenamiento RAID
- [NEW.SW.5.3.6] Se controla la realización de copias de seguridad del código fuente
- [NEW.SW.5.3.7] El código fuente no está accesible en los sistemas en producción
- [H.IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios
- [D.DS.5.1] No reconocidos
- [IP.BS.4.5] Se previene la reinstalación no autorizada de configuraciones previas
- [SW.CM.c] Se retienen copias de las versiones anteriores de software como medida de precaución para contingencias
- [IP.BS.5] Se establece un plan de contingencia específico
- [AUX.AC.2] Sistema de climatización redundante

- [PS.cont.4] El personal alternativo está sujeto a las mismas garantías de seguridad que el habitual
- [G.exam.3.1] Revisión por un equipo de auditoría interna
- [G.exam.3.2] Revisión por un auditor / empresa especializado e independiente
- [L.7.7.1] El personal recibe información específica (obtención de información, respuesta a la amenaza, etc.)
- [H.tools.DLP.8] Disparo de alarmas en tiempo real
- [S.TW.5] Se verifica regularmente que se cumple la política
- [PS.5.1.3] Periódicamente se vuelve a comprobar para el caso de personal con puestos de gran responsabilidad
- [L.AC.3.4] Se revisa regularmente el registro de visitas
- [H.AC.5.5] Se registra el uso de las utilidades
- [D.2.1.3] El nivel de clasificación se mantiene cuando la información se transfiere
- [H.tools.DLP.9] Se emplea un producto certificado o acreditado
- [H.AU.4.1.1.8] Estudio de cambios en las etiquetas de los recursos
- [H.tools.DLP.7.1] Se monitorizan los datos transferidos al exterior (otras redes)
- [H.tools.DLP.7.2] Se monitorizan los datos transferidos a portátiles
- [H.tools.DLP.7.3] Se monitorizan los datos transferidos a PDAs
- [H.tools.DLP.7.4] Se monitorizan los datos transferidos a soportes removibles
- [SW.op.6.2.1] Controles de sesión o de lotes, para conciliación de cuadres de ficheros tras las actualizaciones de transacciones
- [SW.op.6.2.2.1] Controles de pasada en pasada
- [SW.op.6.2.2.2] Totales de actualización de ficheros
- [SW.op.6.2.2.3] Controles de programa a programa
- [SW.op.6.2.3] Validación de los datos generados por el sistema
- [SW.op.6.2.5] Hash de registros y ficheros
- [SW.op.6.2.6] Comprobaciones que aseguren que los programas de las aplicaciones se ejecutan en el momento adecuado
- [SW.op.6.2.7] Comprobaciones que aseguren que los programas se ejecutan en el orden correcto, que finalizan en caso de fallo y que no sigue el proceso hasta que el problema se resuelve
- [BC.DRP.7.1] Las pruebas incluyen varios escenarios
- [HW.op.3.3.4] Se revisa regularmente la relación de equipos ausentes
- [S.TW.4] Se detectan casos de uso inaceptable
- [HW.PCD.8.2] Se instalan detectores de violación
- [PS.cont.2] Se monitorizan continuamente los incidentes de disponibilidad de personal
- [PS.4.3] Se han determinado las responsabilidades en materia de seguridad de los puestos de trabajo
- [PS.4.4] Se tienen en cuenta los requisitos de seguridad de los puestos de trabajo
- [H.tools.DLP.6.1] Registro de actividad no autorizada
- [H.tools.DLP.6.2] Aviso al responsable de la información

- [H.tools.DLP.6.3] Retención cautelar de los datos (cuarentena)
- [G.exam.5] Certificación o acreditación del sistema
- [D.TS.7] Se revisan regularmente las vulnerabilidades de los algoritmos
- [S.TW.2.1] Se ha definido la política de uso aceptable
- [S.TW.6.5] Gestión de incidentes
- [BC.1.1.5.4] Proceso de recuperación (DRP)
- [H.IR.5.8.2] Las evidencias recogidas se almacenan de forma segura
- [H.IR.5.8.3.1] Consta el autor del documento
- [H.IR.5.8.3.2] Constan los testigos del incidente reportado
- [H.IR.5.8.3.3] Se toman medidas para prevenir la alteración del documento
- [H.IR.5.8.4.1] Consta el origen de la evidencia
- [H.IR.5.8.4.2] Se realizan copias en medios de alta fiabilidad
- [H.IR.5.8.4.3] Se registran todas las acciones del proceso de copia
- [H.IR.5.8.4.4] Se dispone de testigos del proceso de copia
- [MP.IC.7] Se tienen en cuenta los requisitos de control de los mecanismos criptográficos (registro, contabilidad, auditoría, etc.)
- [SW.op.6.3.1] Validaciones de verosimilitud para comprobación de los datos de salida
- [SW.op.6.3.2] Cuentas de control de conciliación para asegurar el proceso de todos los datos
- [SW.op.6.3.3] Suministro de suficiente información al lector o a un sistema de proceso subsiguiente para poder determinar la exactitud, completitud, precisión y clasificación de la información
- [K.comms.2] Se dispone de procedimientos de gestión de claves
- [PS.4.6] Se mide el desempeño efectivo, en materia de seguridad, del personal asignado al puesto
- [E.1.1] Se define la propiedad de la información y del software
- [E.1.2] Se definen responsabilidades de custodia
- [E.1.5] Se definen responsabilidades en materia de legislación
- [E.1.6] Se definen responsabilidades para el control y notificación del envío, transmisión y entrega
- [E.1.7] Se definen responsabilidades y obligaciones en caso de incidente de seguridad
- [E.1.8] Se protege el derecho de auditar directamente o por terceros el cumplimiento de las responsabilidades contractuales
- [E.1.f] Se dispone de procedimientos para la notificación del envío, transmisión y recepción
- [E.1.g] Se dispone de procedimientos que aseguren la trazabilidad y el no repudio
- [E.1.h] Se determinan los estándares técnicos adecuados para el encapsulado de la información y su transmisión
- [E.1.i] Se dispone de normativa para la identificación del mensajero
- [E.1.k] Se dispone de normativa para la grabación y lectura de información y software
- [G.plan.1.7] Se estiman las necesidades de personal

- [L.7.3.6] Se realizan pruebas regularmente y se actualizan los procedimientos según los resultados
- [H.AU.2.2.1] Sincronización durante el arranque del sistema
- [L.7.7.6] Se dispone de normativa para la detección de artefactos explosivos
- [L.7.2.j] Se realizan regularmente simulacros con las fuerzas de ayuda exterior
- [SW.1.4] Se identifica el propietario (persona responsable)
- [SW.1.5] El inventario se actualiza regularmente
- [SW.CM.4.3] Se evalúa el impacto en la integridad de los datos
- [H.VM.2.1] de los algoritmos criptográficos
- [H.AC.7.8] Se mantiene un registro de los privilegios de acceso
- [H.AU.3.2.2.6] Se registran los programas y utilidades usados
- [H.AU.3.2.2.9.1] Cambios en permisos y privilegios de usuarios y grupos
- [H.AU.3.2.2.9.2] Cambios en la información relevante de gestión de la seguridad del sistema (incluyendo las funciones de auditoría)
- [H.AU.3.2.2.9.3] Arranque y parada de las funciones (servicios) de auditoría
- [H.AU.3.2.2.9.4] Accesos a la información de seguridad del sistema
- [H.AU.3.2.2.9.5] Borrado, creación o modificación de los registros de auditoría
- [H.AU.3.2.2.9.6] Cambios en la fecha y hora del sistema
- [D.TS.2.1] Procedimiento de fechado
- [D.TS.2.2] Procedimiento de verificación de fecha
- [S.TW.1] Se ha designado al responsable de la administración del servicio
- [S.TW.2.4] Se establecen límites al uso privado
- [S.TW.2.5] Se dispone de normativa relativa al acceso de visitantes y familiares al equipamiento e información
- [S.TW.3.1] uso correcto
- [S.TW.3.2] abuso del servicio
- [S.TW.3.3] riesgos del servicio
- [S.TW.3.4] procedimientos de gestión de incidentes
- [S.TW.7] Se aplican medidas disciplinarias en caso de incumplimiento
- [S.CM.b] Se realizan pruebas de regresión
- [COM.CM.f.1] Se documentan todos los cambios
- [MP.IC.6] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [L.1.1] Se dispone de normativa relativa a la protección de las instalaciones
- [PS.AT.5.3] Cuando se requiere por cambios en el sistema
- [PS.AT.5.4] Reforzamiento regular
- [H.IR.d.4] Cada acción de emergencia es aprobada por la Dirección
- [H.IR.f.1] Se han definido indicadores para la cuantificación y monitorización de los incidentes
- [BC.1.1.5.2] Pruebas y simulacros

- [BC.2.1] Cuando entran nuevos sistemas de información en producción
- [BC.2.2] Cuando se retiran sistemas de información de producción
- [BC.BIA.1] Se identifican y priorizan los procesos críticos
- [BC.BIA.2] Se identifican los activos involucrados en los procesos críticos
- [BC.BIA.3] Se establecen objetivos de recuperación para cada proceso crítico (RTO)
- [BC.BIA.4] Se establecen objetivos de recuperación para cada información crítica (RPO)
- [BC.BIA.5] Se identifican eventos posibles y su potencialidad de producir una interrupción
- [BC.BIA.6] Se identifican los impactos en términos de tiempo de interrupción, daños y tiempo de recuperación
- [BC.DRP.3.2] Los planes se mantienen al día dentro de un proceso de mejora continua
- [BC.DRP.4.1] Se dispone de un procedimiento de notificación
- [BC.DRP.4.2] Se dispone de un procedimiento de activación del plan
- [BC.DRP.6] Se ejecuta un plan de formación
- [BC.7.2] Se evalúa el proceso de retorno al terminarlo
- [G.exam.6.2] Tras efectuar cambios significativos
- [S.3.2.a] Se definen las responsabilidades en la supervisión del cumplimiento del contrato
- [S.TW.9.4.6] Se registra de actividad
- [NEW.SW.5.7.3] Se establecen requerimientos contractuales sobre calidad del código
- [NEW.SW.5.7.4] Se establece un protocolo de revisión del SW desarrollado
- [NEW.SW.5.7.5] La calidad y exactitud del trabajo realizado se certifica según los estándares requeridos
- [E.1.9] Se establecen restricciones en la copia o divulgación de la información
- [E.1.j] Se determina un sistema de etiquetado adecuado para la información sensible o crítica
- [H.tools.DLP.1] Se requiere autorización previa para su utilización
- [H.tools.DLP.2] La herramienta se actualiza regularmente
- [H.tools.DLP.3] Es posible recopilar, mostrar y analizar diferentes tipos de formatos de datos
- [H.tools.DLP.4] Permite crear y aplicar filtros de captura para establecer qué tipos de datos deben recopilarse
- [H.AC.9.1.1] El propietario del recurso puede determinar los derechos de acceso de los demás a su recurso
- [H.AC.9.1.2] Solamente el propietario del recurso puede establecer y modificar los derechos de acceso a su recurso
- [COM.C.5] Se revisan regularmente las vulnerabilidades de los algoritmos
- [S.CM.d.1] Se documentan todos los cambios

- [SW.CM.1.1] Se han designado responsables para autorizar un cambio
- [HW.CM.g.1] Se documentan todos los cambios
- [D.DS.a] Se emplean productos o servicios certificados o acreditados
- [PS.AT.6] Se dispone de un registro de las actividades de formación y concienciación
- [SW.op.6.2.8] Se registran las actividades realizadas
- [SW.op.6.3.6] Se registran las actividades realizadas
- [D.2.2.1] El sistema mantiene los atributos de seguridad íntimamente ligados a la información almacenada, en proceso y transmitida
- [D.2.2.2] Los atributos de seguridad se mantienen asociados a la información cuando ésta se intercambia con otros sistemas
- [D.TS.1.6] Se dispone de normativa de adquisición de productos o contratación de servicios
- [K.comms.a.1] Se dispone de normativa: periodos y condiciones
- [K.comms.a.2] Se definen roles y responsabilidades
- [K.comms.a.3] Se han designado responsables
- [K.comms.a.4] Se dispone de normativa para la recuperación de claves
- [S.3.2.4] Se define, y se incorpora al contrato el procedimiento para medir el cumplimiento de las medidas de seguridad
- [S.3.2.5] IPR: Se contemplan los temas relativos a propiedad intelectual
- [S.3.2.9] Se definen las responsabilidades sobre instalación y mantenimiento de HW y SW
- [S.3.3.1] Se analiza continuamente el nivel de riesgo
- [SW.CM.4.2] Se evalúa el impacto en la confidencialidad de los datos
- [SW.CM.4.4] Se evalúa el impacto en los controles de monitorización
- [PS.4.2] Se especifican las funciones de los puestos de trabajo
- [PS.4.7] Se revisa periódicamente la especificación del puesto
- [BC.DRP.5.1] Están detalladas las actividades de recuperación
- [BC.DRP.5.2] Están detallados los procedimientos de recuperación
- [H.AC.c.1] Concienciación de los usuarios
- [SW.SC.8] La aplicación del perfil se revisa periódicamente
- [H.AC.8.2] Se supervisan las actuaciones del personal que hace cumplir los controles
- [H.AC.8.5] Se investiga toda actividad inusual
- [H.tools.VA.9] Se emplea un producto certificado o acreditado
- [HW.op.3.3.1] Se dispone de un registro de activos fuera de las instalaciones en cada momento
- [HW.op.3.3.2] Se registra la salida
- [HW.op.3.3.3] Se registra el retorno
- [NEW.SW.5.3.5] El acceso al código fuente queda registrado
- [H.IR.2.1.5] Se realizan revisiones periódicas de software y ficheros no autorizados
- [E.1.l] Se revisa regularmente el cumplimiento de acuerdos y contratos

- [COM.C.6] Se emplean algoritmos certificados / acreditados
- [S.TW.2.2] Se tiene en cuenta el marco legal
- [S.TW.2.3] Se tiene en cuenta la política interna
- [S.TW.6.1] Establecimiento de la seguridad física
- [S.TW.6.2] Provisión de equipamiento y mobiliario de almacenamiento
- [S.TW.6.3] Provisión de hardware y software
- [S.TW.6.4] Provisión de comunicaciones incluyendo métodos de acceso remoto seguro
- [S.TW.6.6] Procedimientos de backup y continuidad
- [S.TW.6.7] Procedimientos de auditoría y monitorización de seguridad
- [S.TW.6.8] Procedimientos de devolución del equipamiento y revocación de los derechos de acceso al cesar las actividades
- [S.TW.6.9] Se dispone de un procedimiento de actuación en caso de incumplimiento
- [S.CM.e] Se actualizan todos los procedimientos de producción afectados
- [SW.op.5.1] Se ha identificado el nivel de sensibilidad de la información
- [SW.op.5.2] Se identifican los recursos compartidos y se requiere autorización del responsable
- [SW.CM.2.1] Se sigue un procedimiento formal de autorización de cambios
- [HW.CM.h] Control de versiones de todo cambio de hw
- [HW.PCD.2] Se requiere autorización previa antes de poder usarlos
- [HW.PCD.3] Cada equipo se marca con el nivel máximo de información que puede almacenar o procesar
- [HW.PCD.4] Se han identificado los riesgos correspondientes
- [HW.PCD.5.1] Se ha establecido en qué entornos se puede usar el equipo y cómo
- [HW.PCD.5.2] Se ha establecido a qué redes se puede conectar el equipo y cómo
- [HW.PCD.5.3] Se ha establecido qué periféricos se pueden conectar el equipo y cómo
- [COM.CM.f.2] Se actualiza la documentación del sistema
- [H.IR.e.4] Se prueban regularmente los procedimientos de gestión de incidentes
- [BC.1.1.5.1] Planificación
- [BC.1.1.5.3] Gestión de crisis
- [H.AU.4.2] Consolidación y reporte
- [S.3.3.7] Se definen procedimientos para notificar e investigar los incidentes y fallos de seguridad
- [L.6.3.6] Periódicamente se comprueba que funciona adecuadamente
- [MP.4.3.4] Se requiere confirmación de entrega
- [D.DS.9] Se emplean algoritmos certificados / acreditados

- [MP.4.3.7.3] Se monitorizan las discrepancias entre envíos y recepciones
- [MP.4.3.7.4] Se monitorizan los tiempos excesivos entre envío y recepción
- [H.AC.6.1] Se requiere autorización previa para el acceso a la configuración sistema
- [H.ST.3.2] Se monitorizan todas las operaciones
- [S.CM.d.2] Se actualiza la documentación del sistema
- [SW.op.6.3.4] Procedimientos para contestar los cuestionarios de validación de salidas
- [SW.op.6.3.5] Se han definido las responsabilidades de todos los implicados en el proceso de salida de datos
- [HW.CM.g.2] Se actualiza la documentación del sistema
- [L.6.4.1] espectro visible
- [L.6.4.2] infrarrojos
- [H.AC.2.1] Procedimiento de concesión de privilegios
- [PS.8.1.1] virus
- [BC.DRP.2] Todas las áreas de la organización están coordinadas
- [H.AC.6.4] Se registra el acceso a la configuración del sistema
- [BC.2.3] Cuando entran servicios en producción
- [BC.2.4] Cuando hay cambios en los servicios
- [BC.2.5] Cuando se retiran servicios de producción
- [BC.2.c] Cuando entran en producción servicios de comunicaciones
- [BC.2.d] Cuando hay cambios en los servicios de comunicaciones
- [BC.2.e] Cuando se retiran servicios de comunicaciones de producción
- [BC.2.9] Cuando entra equipamiento (HW) en producción
- [BC.2.a] Cuando hay cambios en el equipamiento (HW)
- [BC.2.b] Cuando se retira equipamiento (HW) de producción
- [BC.2.6] Cuando entran aplicaciones (SW) en producción
- [BC.2.7] Cuando hay cambios en las aplicaciones (SW)
- [BC.2.8] Cuando se retiran aplicaciones (SW) de producción
- [BC.2.f] Cuando se estrenan nuevas instalaciones
- [BC.2.g] Cuando hay cambios en las instalaciones
- [BC.2.h] Cuando se cierran instalaciones
- [BC.2.i] Cuando hay cambios en el personal adscrito
- [MP.4.1.4] Se realizan revisiones periódicas de las listas de distribución y destinatarios autorizados
- [MP.5.3.4] Se revisa regularmente la relación de soportes ausentes
- [H.tools.DLP.5] Permite crear y aplicar filtros de presentación para establecer qué tipos de datos deben mostrarse
- [H.AC.8.3] Se revisan regularmente los registros de actividad en busca de acciones inapropiadas
- [H.AC.8.4] Se registran y se revisan regularmente los cambios en las autorizaciones de acceso
- [H.AU.4.1.1.1] Intentos de acceso fallidos
- [H.AU.4.1.1.3] Cuentas usadas fuera del horario normal
- [H.AU.4.1.1.4] Estadísticas sobre uso de cuentas

- [H.AU.4.1.1.5] Estadísticas sobre accesos remotos
- [H.AU.4.1.1.6] Identificación de transacciones
- [S.1.2.2] Se detectan casos de uso inaceptable
- [S.1.2.3] Se verifica regularmente que se cumple la política
- [COM.wifi.8] Se comprueban periódicamente los puntos de acceso (mediante broadcast o herramientas)
- [NEW.SW.5.3.3] Se requiere autorización previa para la actualización y entrega de código fuente a programadores
- [NEW.SW.5.3.4] Se protegen físicamente los listados de programas
- [NEW.SW.5.8.2] Existe una descripción detallada de funciones y procedimientos
- [S.3.2.8] Se describen los servicios disponibles
- [PS.5.3.1] Entrevista previa a la finalización
- [MP.clean.5.2] Se emplea un producto o servicio certificado o acreditado
- [H.AU.2.2.5.1] Sincronización automática con un reloj propio centralizado
- [SW.op.6.1.1.1] Comprobación del rango de valores
- [SW.op.6.1.1.2] Comprobación del tipo de datos de entrada
- [SW.op.6.1.1.3] Comprobación de la completitud de los datos de entrada
- [SW.op.6.1.1.4] Comprobación del volumen de datos
- [SW.op.6.1.1.5] Comprobación de datos no autorizados o inconsistentes
- [SW.op.6.1.2] Comprobación de la integridad de los datos mediante revisión periódica de campos clave o ficheros de datos
- [SW.op.6.1.3] Inspección de los documentos físicos de entrada para ver si hay cambios no autorizados
- [SW.op.6.1.5] Se verifica la plausibilidad de los datos de entrada
- [L.7.4.1] Se han identificado los posibles accidentes naturales
- [L.7.4.2] Se han identificado los posibles accidentes industriales
- [L.AC.2.6] El registro de accesos se revisa periódicamente
- [SW.op.6.2.4] Comprobaciones de integridad de datos o del software transferidos desde o hacia el ordenador central
- [L.7.2.c] Se dispone de un sistema automático de detección de incendios
- [H.AC.3] Se definen y documentan las autorizaciones de acceso
- [H.AU.1.1.1] Se tienen en cuenta los requisitos legales y contractuales
- [H.AU.1.1.2] Se han establecido criterios para garantizar que las pruebas son admisibles
- [H.AU.1.1.3] Se han establecido criterios sobre la calidad y completitud de las pruebas
- [H.AU.1.1.4] La norma para el registro de eventos especifica las necesidades de retención
- [H.AU.1.1.5] La norma para el registro de eventos especifica las necesidades y derechos de acceso

- [H.AU.1.1.6.1] clientes y servidores en arquitecturas orientadas a servicios
- [H.AU.1.1.6.2] servicios públicos de seguridad
- [H.AU.1.2.1] Se planifican los requisitos y las actividades de auditoría
- [H.AU.1.2.2] Se planifican las necesidades de almacenamiento y proceso
- [COM.C.1.1] Se tienen en cuenta los requisitos legales y contractuales
- [COM.C.1.2] Se definen roles y responsabilidades
- [COM.C.1.3] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [COM.C.1.4] Se tienen en cuenta los requisitos de control: registro y auditoría
- [COM.C.1.5] Se dispone de normativa de adquisición de productos
- [COM.C.1.6] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [COM.C.2] Se han designado responsables
- [L.cont.1] Se analizan las implicaciones para la continuidad del negocio
- [L.cont.2] Se establece un protocolo de actuación en caso de contingencia
- [H.AU.3.3.6] Los diarios de operaciones se revisan regularmente por otro responsable
- [D.C.4.3] Se emplean algoritmos certificados / acreditados
- [IP.1.3] Se realiza una monitorización continua de las conexiones autorizadas
- [MP.5.6] El soporte se revisa a su regreso
- [MP.end.6.2] Se emplea un producto o servicio certificado o acreditado
- [L.AC.2.b.4] Periódicamente se revisa y se realizan las actividades de mantenimiento
- [L.AC.c.9] Periódicamente, se realiza un auditoría
- [H.ST.3.c] Se revisan los periodos de vacaciones previstos
- [H.IR.c.3] Se revisan las medidas correctoras para comprobar que son efectivas
- [H.ST.3.1] Se registran todas las operaciones
- [D.1.1] Se dispone de un registro de activos de información
- [D.1.2] Se identifica al propietario (persona responsable)
- [D.1.3] El inventario se actualiza regularmente
- [COM.DS.1.4] Se monitoriza el punto de interconexión
- [COM.SC.8] La aplicación del perfil se revisa periódicamente
- [H.VM.4.1] daños sobre la misión o negocio del sistema
- [H.VM.6.2] medidas de emergencia ante riesgos elevados
- [S.TW.2.6] IPR: Se establecen los términos de propiedad intelectual de los trabajos realizados
- [COM.CM.f.3] Se destruye o se archiva la documentación anterior

- [PS.5.3.3] Comunicación de la baja a los responsables de seguridad, y administradores del sistema
- [D.backup.1.2] El acceso a las copias de seguridad requiere autorización previa
- [COM.CM.h] Se actualizan todos los procedimientos de recuperación afectados
- [MP.IC.9.3] Se emplean algoritmos certificados / acreditados
- [SW.CM.4.1] Se evalúa el impacto en la prestación de los servicios
- [H.AU.2.2.2] Se comprueba periódicamente la sincronización
- [H.AU.2.2.4] Comprobación tras actualizaciones de software, o cambios de configuración
- [H.AU.2.2.6] Los usuarios no pueden cambiar los relojes de sus estaciones
- [S.op.1.3] Se dispone de un registro de transacciones / transmisiones
- [L.AC.2.5] Se mantiene un registro de los accesos
- [HW.6.1.1] Se tienen en cuenta los requisitos de identificación y autenticación
- [HW.6.1.2] Se tienen en cuenta los requisitos de aplicabilidad (confidencialidad, integridad, autenticidad y no repudio)
- [HW.6.1.3] Se tienen en cuenta los requisitos legales y contractuales
- [HW.6.1.4] Se definen roles y responsabilidades
- [HW.6.1.5] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [HW.6.1.6] Se tienen en cuenta los requisitos de control de los mecanismos criptográficos (registro, contabilidad, auditoría, etc.)
- [HW.6.1.7] Se dispone de normativa de adquisición
- [HW.6.1.8] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [S.3.3.6] Se definen responsabilidades y procedimientos para notificar y gestionar los incidentes de seguridad
- [S.3.3.9] Se establece un procedimiento de escalado para la resolución de incidentes
- [NEW.SW.4.2] Se usan productos certificados / evaluados
- [D.backup.2.1.1] Se identifica la información crítica para el negocio
- [D.backup.2.1.2] Se establece la frecuencia de las copias
- [D.backup.2.1.3] Se definen roles y funciones en relación a las copias de seguridad
- [D.backup.2.1.4] Se dispone de normativa para la realización de copias
- [D.backup.2.1.5] Se dispone de normativa para la restauración de datos
- [D.backup.2.1.6] Se dispone de normativa para la retención y destrucción de copias de seguridad
- [D.backup.2.1.7] Se establecen los requisitos de almacenamiento en el propio lugar, y en lugares alternativos
- [D.backup.2.2.1] Procedimiento de realización de copias
- [D.backup.2.2.2] Procedimiento de restauración de datos

- [D.backup.2.2.3] Procedimiento almacenamiento local de copias
- [D.backup.2.2.4] Procedimiento almacenamiento remoto de copias
- [D.backup.2.2.5] Procedimiento de eliminación de copias que ya no son necesarias
- [H.tools.TM.8] Disparo de alarmas en tiempo real
- [H.tools.TM.9] Se emplea un producto certificado o acreditado
- [H.tools.AV.b] Se emplea un producto certificado o acreditado
- [H.AU.3.5] Los registros se fechan
- [D.C.4.2] Se revisan regularmente las vulnerabilidades de los algoritmos
- [D.DS.8] Se revisan regularmente las vulnerabilidades de los algoritmos
- [HW.op.3.7] El activo se revisa a su regreso
- [PS.AT.4.1] Previa al uso de los sistemas
- [PS.AT.5.2] Previa al acceso a los sistemas
- [H.IR.f.2] Se actualizan los procedimientos de usuario para incorporar o mejorar la identificación y forma de reaccionar ante el mismo incidente o incidentes similares
- [H.IR.f.3] Se actualizan, extienden, mejoran u optimizan los procedimientos de resolución de incidentes
- [S.CM.d.3] Se archiva o se destruye la documentación anterior
- [HW.CM.g.3] Se destruye o se archiva la documentación anterior
- [MP.4.3.6.3] Uso de contenedores con detección de apertura
- [MP.IC.9.2] Se revisan regularmente las vulnerabilidades de los algoritmos
- [D.2.1.1.1] Se han establecido clases y directrices de clasificación
- [D.2.1.1.5] la responsabilidad de la clasificación / reclasificación es del propietario (responsable) de la información
- [H.IR.3] El personal designado cubre las 24h los 7 días de la semana
- [H.IR.2.1.4] Se realizan revisiones periódicas de software, datos y sistemas críticos
- [H.IR.2.f] Coordinación con otros sistemas de información afectados
- [H.IR.5.3.1] Daños sobre la misión o negocio del sistema
- [H.IR.5.8.1] Se recogen pistas de auditoría, atendiendo a su validez, calidad y completitud
- [H.IR.d.3] Queda registro de todas las acciones realizadas
- [COM.C.7] Se emplean productos o servicios certificados o acreditados
- [H.IR.2.1.8] Los planes de continuidad tienen en cuenta posibles infecciones por código dañino
- [AUX.1.1] Se dispone de un registro de equipamiento auxiliar
- [AUX.1.2] Se identifica el propietario (persona responsable)
- [AUX.1.3] El inventario se actualiza regularmente
- [AUX.1.4] Se registran las entradas y salidas de equipamiento auxiliar
- [S.CM.f] Se actualizan todos los procedimientos de recuperación afectados

- [H.AU.2.2.3] Comprobación tras el cambio de horario (verano e invierno - DST)
- [H.AC.8.1.3] Se revisan al causar baja
- [H.AC.a.b] Se presenta un mensaje indicando el uso debido del sistema
- [H.AC.a.c] Se presenta un mensaje indicando que queda prohibido todo uso no autorizado
- [H.AC.a.d] Se presenta un mensaje indicando que toda la actividad podrá ser supervisada
- [H.AC.a.e] Tras la conexión, se muestra la fecha y hora de la anterior conexión realizada con éxito
- [H.AC.a.f] Tras la conexión, se muestran los intentos fallidos
- [H.VM.1] Se dispone de personas dedicadas a la gestión de vulnerabilidades
- [H.AU.4.1.2] Se revisa al menos cada mes
- [K.comms.1.1] Se identifica el uso autorizado de cada clave
- [K.comms.1.2] Se cubre la puesta en operación de nuevas claves
- [K.comms.3] Se identifica la persona responsable de cada clave
- [S.1.2.4.1] uso correcto
- [S.1.2.4.2] abuso del servicio
- [S.1.2.4.3] riesgos del servicio
- [S.1.2.4.4] procedimientos de gestión de incidentes
- [S.1.2.5] Se dispone de un procedimiento de actuación en caso de incumplimiento
- [S.1.2.6] Se aplican medidas disciplinarias en caso de incumplimiento
- [COM.2] Se dispone de normativa sobre el uso correcto de las comunicaciones
- [COM.3.1] Uso rutinario
- [COM.3.2] Procedimientos específicos de seguridad
- [COM.3.3] Actuación en caso de funcionamiento anómalo
- [MP.3.1] Se mantiene una relación de soportes
- [MP.3.2] Se identifica al propietario (persona responsable)
- [MP.3.3] Se identifica al depositario (o depositarios)
- [MP.3.4] El inventario se actualiza regularmente
- [L.6.5] El personal está concienciado y recibe formación en lo relativo a detección y reacción frente actividades sospechosas en las cercanías del recinto
- [PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)
- [PS.2.2] Se dispone de una relación de personal subcontratado
- [PS.6.1] Se revisan sus requisitos y su satisfacción por el empleado
- [H.IR.5.6.2] externos
- [AUX.wires.5] Se sigue un procedimiento para la modificación del cableado
- [NEW.SW.3.4] Se tienen en cuenta los requisitos de integridad
- [NEW.SW.3.7] Se tienen en cuenta los requisitos de registro
- [D.backup.2.4.1.1.1] Se identifica por medio de un código único

- [D.backup.2.4.1.1.2] Consta la fecha de creación
- [D.backup.2.4.1.1.3] Consta la fecha de caducidad
- [D.backup.2.4.1.1.4] Consta el período de retención
- [D.2.1.2] Se dispone de procedimientos para el tratamiento de información clasificada
- [H.AC.8.1.1] Se revisan regularmente a intervalos marcados por la normativa
- [S.3.3.8] Se definen formatos y medios de reporte
- [H.VM.6.3] plan de actuación frente a riesgos moderados
- [D.TS.1.2] Se tienen en cuenta los requisitos de custodia de evidencias
- [S.3.3.5] Se establecen controles de monitorización y verificación del rendimiento
- [MP.4.4] Formación del personal en gestión de soportes
- [PS.5.2.5.3] Difusión del procedimiento
- [H.IR.e.3.5] Incidentes ocurridos
- [PS.4.5.3] ... de tratamiento de datos clasificados
- [H.tools.VA.6] Es posible seleccionar o deseleccionar uno o más subconjuntos de vulnerabilidades
- [H.tools.VA.7] Es posible configurar reglas de autenticación y acceso que sólo permitan utilizar la herramienta a los usuarios autorizados
- [H.tools.VA.8] Es posible producir informes en varios formatos y siguiendo distintos criterios
- [L.AC.4.1] Se dispone de procedimientos para la emisión, control, registro, baja y cancelación de los pases
- [L.AC.4.2] Se requiere que la identificación de las personas sea visible
- [S.3.2.3.2] En lo relativo a integridad de la información
- [S.3.2.3.4] En lo relativo a autenticidad
- [S.3.2.3.5] En lo relativo a trazabilidad
- [E.1.4] IPR: Se definen responsabilidades sobre protección de la propiedad intelectual / industrial
- [S.2.9.6] Se dispone de un registro de actividades
- [H.AU.3.2.4] En arquitecturas orientadas a servicios, se retiene suficiente información para coordinar los registros en el cliente y en el servidor
- [MP.4.2.1] Se dispone de normativa para el etiquetado y cambio de etiquetas
- [MP.4.2.2] Se dispone de procedimientos para el etiquetado y cambio de etiquetas
- [MP.4.2.3] Se marcan todos los soportes indicando la clasificación de la información que contienen o pueden contener
- [MP.4.2.4.1] El contenedor se etiqueta al máximo nivel de clasificación de la información que contenga
- [MP.4.2.4.2] La etiqueta no proporciona ninguna información sobre su contenido
- [MP.4.2.5] La etiqueta sólo permite conocer el nivel de clasificación, no la información

- [MP.4.2.6] Los usuarios disponen de medios y formación para interpretar correctamente lo significado por las etiquetas
- [MP.4.3.7.1] Se registran los envíos de soportes
- [MP.4.3.7.2] Se registran las recepciones de soportes
- [L.1.2] Se han establecido normas de conducta (prohibición de fumar, beber, comer, ...)
- [IP.SPP.4.3] Se realiza una monitorización continua del tráfico
- [L.7.3.5] Se dispone de normativa de reacción en caso de emergencia
- [H.IR.a.1.1] Se han definido criterios para interpretar síntomas y mensajes que aparezcen en pantalla
- [H.IR.a.1.2.1] ¿A quién se debe informar?
- [H.IR.a.1.2.2] ¿Qué datos se deben registrar?
- [H.IR.a.1.2.3] ¿Qué se debe hacer con el sistema que falla?
- [IP.BS.2.8] La aplicación del perfil se revisa periódicamente
- [IP.1.5] Se revisan regularmente los usuarios y procesos autorizados
- [COM.aut.4.2.3] Se usa un producto certificado o acreditado
- [IP.SPP.4.6] Se revisan periódicamente las trazas de actividad
- [H.VM.2.2] de los servicios prestados
- [S.CM.5.3] Se evalúa el impacto en la integridad de los datos
- [NEW.S.2.4] Se tienen en cuenta los requisitos de integridad
- [NEW.S.2.7] Se tienen en cuenta los requisitos de trazabilidad (accounting)
- [D.2.1.1.3] los niveles de clasificación se han definido considerando las necesidades de conocer y de compartir
- [D.2.1.1.6] Existe normativa de control de acceso
- [D.2.1.1.7.1] cópias impresas
- [D.2.1.1.7.2] copias electrónicas
- [D.2.1.1.8.1] impresas
- [D.2.1.1.8.2] electrónicas
- [D.2.1.1.9] Existe normativa de etiquetado de soportes de información
- [D.2.1.1.a] Existe normativa de transmisión telemática
- [D.2.1.1.b] Existe normativa de transporte físico de información clasificada
- [D.2.1.1.c.1] impresas
- [D.2.1.1.c.2] electrónicas
- [D.2.1.1.d] Existe normativa de empleo de productos certificados o acreditados
- [COM.DS.1.1] La segregación atiende a los requisitos de control de acceso
- [H.AU.4.1.1.2] Cuentas con privilegios especiales
- [H.AU.4.1.1.7] Estadísticas de impresión
- [L.AC.3.3] Se mantiene un registro de entrada / salida (nombre, empresa, fecha y horas de entrada y salida, objeto del acceso, y persona que recibe)
- [SW.1.1] Se dispone de un registro de aplicaciones
- [SW.1.2] Se dispone de un registro de software de base

- [SW.1.3] Se dispone de un registro de sistemas operativos
- [HW.CM.5.3] Se evalúa el impacto en la integridad de los datos
- [COM.CM.e] Todas las actuaciones quedan registradas
- [NEW.S.2.6] Se tienen en cuenta los requisitos de autenticidad
- [NEW.HW.2.4] Se tienen en cuenta los requisitos de integridad
- [NEW.COM.2.6] Se tienen en cuenta los requisitos de autenticidad
- [NEW.COM.2.7] Se tienen en cuenta los requisitos de trazabilidad (accounting)
- [G.2.2.9] Se realizan pruebas de aceptación
- [NEW.SW.5.8.1] Se dispone del código fuente
- [L.7.2.b] Se dispone de pulsadores de alarma
- [H.IR.2.1.1] Están definidas las responsabilidades en la gestión de código dañino
- [H.IR.2.1.2] Están definidas las medidas de protección contra código dañino
- [H.AC.4.1] Se requiere autorización previa
- [H.AC.4.2] Se requiere que haya necesidad de conocer
- [H.VM.2.3] del software base
- [S.2.9.1.2] ... de autenticación
- [COM.op.2.2] Revisiones periódicas de la seguridad
- [MP.4.1.5] Quedan registradas las operaciones de creación, modificación y borrado, a efectos de trazabilidad
- [MP.5.3.1] Se dispone de un registro de soportes fuera de las instalaciones en cada momento
- [MP.5.3.2] Se registra la salida
- [MP.5.3.3] Se registra el retorno
- [H.IA.5.4] Las cuentas especiales están sujetas a procesos específicos de gestión
- [H.AC.2.3] Procedimiento de suspensión temporal de privilegios
- [H.AC.2.4] Procedimiento de reactivación de privilegios suspendidos
- [H.AC.7.1] Se identifican los perfiles de acceso y sus privilegios asociados
- [H.AC.7.4] Los derechos de acceso son aprobados por el propietario del servicio o de la información
- [H.AC.7.5] La comunicación de sus derechos a los usuarios consta por escrito
- [H.AC.7.6] Los usuarios reconocen por escrito que conocen y aceptan sus derechos
- [H.AU.3.1] El análisis de riesgos se emplea para determinar lo que se debe registrar
- [H.AU.3.2.1.1] Se identifica el usuario
- [H.AU.3.2.1.2] Se identifica el terminal
- [H.AU.3.2.1.3] Se identifica el proceso
- [H.AU.3.2.1.4] Se registra la fecha y hora
- [H.AU.3.2.1.5] Se registra el tipo de evento
- [H.AU.3.2.1.6] Se registra el resultado del evento (fallo o éxito)
- [H.AU.3.2.2.1] Encendido y apagado del sistema
- [H.AU.3.2.2.2] Inicio y cierre de sesión de usuarios

- [H.AU.3.2.2.3] Intentos de inicio de sesión
- [H.AU.3.2.2.4] Intentos aceptados y rechazados de acceso a datos y otros recursos
- [H.AU.3.2.2.5] Se registran los accesos a ficheros
- [H.AU.3.2.2.7] Se registran las operaciones sobre datos y aplicaciones
- [H.AU.3.2.2.8] Se registran las impresiones realizadas
- [H.AU.3.3.1] Se registran las actividades del personal de administración
- [H.AU.3.3.2] Se registran los tiempos de arranque y parada del sistema
- [H.AU.3.3.3] Se registran los errores del sistema y de las operaciones para su corrección
- [H.AU.3.3.4] Se registra la confirmación del manejo correcto de los ficheros de datos y los resultados
- [H.AU.3.3.5] Se registra el nombre de quien realiza la entrada en el diario
- [H.AU.3.8] Se retienen los registros durante el periodo establecido por política
- [D.C.1.1] Se tienen en cuenta los requisitos legales y contractuales
- [D.C.1.2] Se definen roles y responsabilidades
- [D.C.1.3] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [D.C.1.4] Se tienen en cuenta los requisitos de control: registro y auditoría
- [D.C.1.5] Se dispone de normativa de adquisición de productos
- [D.C.1.6] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [D.C.2.1] Procedimiento de cifra
- [D.C.2.2] Procedimiento de descifrado
- [D.C.3] Se han designado responsables
- [D.DS.1.1] Se tienen en cuenta los requisitos de identificación y autenticación
- [D.DS.1.2] Se tienen en cuenta los requisitos de no repudio
- [D.DS.1.3] Se tienen en cuenta los requisitos legales y contractuales
- [D.DS.1.4] Se definen roles y responsabilidades
- [D.DS.1.5] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [D.DS.1.6] Se tienen en cuenta los requisitos de control: registro y auditoría
- [D.DS.1.7] Se dispone de normativa de adquisición de productos
- [D.DS.1.8] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [D.DS.2.1] Procedimientos de firma
- [D.DS.2.2] Procedimientos de verificación de firma
- [D.DS.3] Se han designado responsables
- [D.TS.3] Se han designado responsables
- [S.TW.8] Se requiere autorización previa

- [S.3.4.1] Se establece un protocolo formal para la modificación de los servicios prestados
- [S.3.4.2] Se establece un protocolo formal para la gestión de cambios realizados en los sistemas del proveedor
- [SW.2.1] Se dispone de normativa sobre el uso autorizado de las aplicaciones
- [SW.2.2] Se dispone de normativa para la transferencia de SW a otros (organizaciones externas)
- [SW.3.1] Uso rutinario
- [SW.3.2] Procedimientos específicos de seguridad
- [SW.3.3] Actuación en caso de funcionamiento anómalo
- [SW.backup.1.1] Procedimientos de copia
- [SW.op.e] Formación del personal en configuración de aplicaciones
- [HW.1.1] Se dispone de un registro de equipos propios
- [HW.1.3] Se identifica el propietario (persona responsable)
- [HW.1.4] El inventario se actualiza regularmente
- [HW.1.5] Se registran los traslados internos
- [HW.3.1] Uso rutinario
- [HW.3.2] Procedimientos específicos de seguridad
- [HW.3.3] Actuación en caso de funcionamiento anómalo
- [HW.end.1] Se dispone de normativa para la retirada de equipamiento (HW) de producción
- [COM.1.1] Se dispone de un registro de servicios propios
- [COM.1.2] Se dispone de un registro de servicios ajenos
- [COM.1.3] Se identifica el propietario (persona responsable)
- [COM.1.4] El inventario se actualiza regularmente
- [COM.start.1] Se dispone de normativa de entrada en servicio
- [COM.start.2] Se requiere autorización previa
- [COM.start.3] Se revisa la corrección y completitud de la documentación
- [COM.op.1.1.1] Se identifican las redes y los servicios a los que se puede acceder
- [COM.op.1.1.2] Se dispone de normativa relativa a las autorizaciones de acceso a las redes y servicios
- [COM.op.1.1.3] Se dispone de normativa relativa a la protección de los accesos a las redes y servicios
- [COM.op.1.2] Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios
- [COM.CM.1.1] Se han designado responsables para autorizar un cambio
- [COM.CM.4.3] Se evalúa el impacto en la integridad de los datos
- [COM.CM.4.4] Se evalúa el impacto en los controles de monitorización
- [IP.SPP.1] Cualquier otro nodo de la red se considera no fiable, realizándose un control local de los datos intercambiados
- [MP.1.1] Uso de soportes de información
- [MP.1.2] Protección de los soportes en función de la información que contienen

- [MP.1.3] Normativa específica para soportes removibles
- [MP.2] Se dispone de procedimientos relativos a soportes de información
- [MP.IC.1.1] Se tienen en cuenta los requisitos legales y contractuales
- [MP.IC.1.2] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [MP.IC.1.3] Se tienen en cuenta los requisitos de identificación y autenticación
- [MP.IC.1.4] Se tienen en cuenta los requisitos de aplicabilidad (confidencialidad, integridad, autenticidad y no repudio)
- [MP.IC.1.5] Se definen roles y responsabilidades
- [MP.IC.2] Se han designado responsables
- [MP.clean.1] Se dispone de normativa que determina qué información debe ser eliminada de forma segura
- [MP.clean.2] Se dispone de procedimientos para la limpieza de soportes
- [AUX.power.2] Instalación de acuerdo a la normativa vigente
- [L.3.1] Se requiere autorización previa
- [L.AC.2.1] Se dispone de normativa de control de accesos
- [L.AC.2.2] Se dispone de procedimientos para el control de accesos
- [L.AC.2.3] Se definen y documentan las autorizaciones de acceso
- [L.AC.2.7] Se investiga cualquier sospecha o intento de acceso físico no autorizado
- [H.ST.2.a] Se proporciona formación en las funciones de cada rol del sistema
- [PS.5.2.1] Inclusión del ámbito, el alcance y el periodo de las responsabilidades en materia de seguridad
- [PS.5.2.2] Inclusión de obligaciones y derechos legales de ambas partes
- [PS.5.2.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente
- [PS.AT.1] La Política de Seguridad contempla los aspectos de formación y concienciación
- [PS.AT.2] Se dispone de normativa relativa a las actividades de formación y concienciación
- [PS.AT.3] Se dispone de procedimientos relativos a las tareas de formación y concienciación
- [PS.AT.4.2] Cuando se requiere por cambios en el sistema
- [PS.AT.4.3] Reforzamiento regular
- [PS.AT.5.1] Se establecen las necesidades de formación según roles y responsabilidades
- [PS.AT.7] Evaluación y revisión del plan de formación y concienciación
- [PS.8.1.3] otros ...
- [H.IR.1] Se dispone de normativa de actuación para la gestión de incidentes
- [H.IR.5.2] Se identifica y analiza la causa
- [H.IR.5.4] Se planifica la implantación de medidas correctoras

- [H.IR.5.7] Se informa de las acciones a la autoridad respectiva de la organización
- [H.IR.c.1] Se registra toda comunicación sobre fallos en el sistema
- [H.IR.c.4] Se retienen los registros de fallos durante el periodo establecido
- [H.IR.d.1] Se ha identificado el personal que va a gestionar el incidente
- [H.IR.d.2] Se requiere autorización previa del personal que va a gestionar el incidente
- [H.IR.e.2] Formación del personal en detección y gestión de incidentes
- [BC.1.1.1] Están definidos el objeto y el alcance (funciones, procesos y plataformas afectadas)
- [BC.1.1.2] Se dispone de normativa de valoración de daños
- [BC.1.1.3] Información de referencia
- [BC.1.1.4] Se tienen en cuenta los requisitos legales y contractuales
- [BC.DRP.1] Se han designado responsables
- [BC.DRP.3.1] La documentación se aprueba y se garantiza que llegue a los afectados
- [BC.7.1] Se dispone de normativa para la vuelta a la normalidad
- [G.2.1.1.1] Existe una descripción de las areas
- [G.2.1.1.2] Puntos de acceso a las instalaciones
- [G.2.1.2.1] Existe una descripción de las redes internas
- [G.2.1.2.2] Existe una descripción de las conexiones a redes externas
- [G.2.1.2.3] Existe una descripción de las conexiones a Internet
- [G.2.1.3.1.1] Conexiones entre zonas de confianza internas
- [G.2.1.3.1.2] Conexiones a zonas de confianza externas controladas
- [G.2.1.3.1.3] Conexiones a Internet
- [G.2.1.3.2] Esquema de líneas de defensa
- [G.2.1.3.3] Empleo de cortafuegos
- [G.2.1.3.4] Empleo de diodos (comunicaciones unidireccionales)
- [G.2.1.3.5] Empleo de zonas desmilitarizadas (DMZ)
- [G.2.1.3.6] Empleo de productos de diferentes fabricantes
- [G.2.1.4.1] Acceso local: terminales
- [G.2.1.4.2] Acceso local: consolas de administración
- [G.2.1.4.3] Acceso remoto
- [G.2.1.5.1] Mecanismo(s) de identificación
- [G.2.1.5.2] Mecanismo(s) de autenticación
- [G.2.1.5.3] Elementos de verificación de identidad y autenticidad
- [G.2.1.5.4] Mecanismo(s) de control de los derechos de acceso (privilegios)
- [G.3.3.5] Son conocidas y aceptadas por los afectados
- [G.3.4.1] Se revisan regularmente
- [NEW.SW.3.1] Se tienen en cuenta los requisitos de control de acceso
- [NEW.SW.3.2] Se tienen en cuenta los requisitos de identificación y autenticación

- [NEW.SW.3.5] Se tienen en cuenta los requisitos de confidencialidad
- [NEW.SW.3.6] Se tienen en cuenta los requisitos de auditoría
- [L.design.4.2.3] cuentan con detectores de rotura / apertura
- [L.7.2.g] Se notifica automáticamente a los servicios de ayuda exterior de cualquier activación del sistema automático de detección de incendios
- [L.AC.2.c] Se dispone de un sistema de cámaras de vigilancia
- [S.CM.c] Se registran las actualizaciones de servicios
- [COM.cont.4] Se monitorizan enlaces y dispositivos de red
- [G.plan.1.4.1] Dependencia de servicios internos
- [G.plan.1.4.2] Dependencia de servicios externos (proporcionados por otros)
- [AUX.AC.1] Se dimensiona el sistema considerando necesidades futuras
- [SW.op.6.1.4] Se dispone de procedimientos de respuesta ante errores de validación
- [SW.op.6.1.6] Se han definido las responsabilidades de todos los implicados
- [SW.CM.g] Se registra toda actualización de SW
- [NEW.SW.5.7.1] Se realiza un contrato
- [COM.CM.4.2] Se evalúa el impacto en la confidencialidad de los datos
- [H.AC.1.1] Se basa en los requisitos de seguridad y del negocio
- [H.AC.1.2] Se definen los tipos de acceso
- [H.AC.1.3] Se definen los motivos para modificar los derechos de acceso
- [H.AC.1.4] Se revisa regularmente
- [H.AC.5.1] Se requiere autorización previa para el acceso a las utilidades del sistema
- [L.cont.4] Las instalaciones alternativas están sujetas a las mismas garantías de protección que las habituales
- [H.IR.5.5.1] internos
- [H.IR.5.5.2] externos
- [S.3.2.3.3] En lo relativo a confidencialidad de la información
- [G.2.3.2] El propietario del sistema sólo concede acceso a un número restringidos de personas
- [G.2.3.3.3] Garantías de confidencialidad
- [G.2.3.4.2] Garantías de confidencialidad
- [MP.5.3.5.1] Tipo y número de soportes
- [MP.5.3.5.2] Fecha y hora
- [MP.5.3.5.3] Emisor / receptor
- [MP.5.3.5.4] Tipo de información contenida
- [MP.5.3.5.5] Forma de envío
- [MP.5.3.5.6] Identificación del transportista
- [D.TS.8] Se emplean productos o servicios certificados o acreditados
- [IP.SPP.4.4] Se detecta y bloquea el código dañino (malware)
- [H.ST.3.f] Se supervisan las operaciones críticas

- [H.IR.c.2] Se revisan los registros de fallos para asegurar que todos han sido resueltos satisfactoriamente
- [PS.5.2.4.1] Inclusión de cláusulas de confidencialidad en los contratos laborales
- [AUX.wires.4] Todos los elementos de cableado están etiquetados
- [H.IR.2.1.6] Concienciación: ¿cómo actuar frente al código dañino?
- [H.IR.2.1.7] Formación: ¿cómo actuar frente al código dañino?
- [S.CM.2.1] Se han designado responsables para autorizar un cambio
- [SW.CM.h.1] Se documentan todos los cambios
- [HW.CM.1.1] Se han designado responsables para autorizar un cambio
- [G.1.1.1] Está respaldado por la dirección
- [G.1.3.1] Responsable(s) de la información
- [G.1.3.2] Responsable(s) de los servicios
- [G.3.1.6] Se revisa regularmente
- [G.3.2.5] Es conocida y aceptada por los afectados
- [G.2.3.3.2] Garantías de integridad
- [G.2.3.4.1] Garantías de integridad
- [G.2.3.6] Norma de retención de versiones previas
- [S.1.2.1.1] Se ha definido la política de uso aceptable
- [PS.5.2.5.1] Régimen sancionador por incumpliento
- [PS.5.2.4.2] Revisión de las cláusulas de confidencialidad al modificar / expirar los contratos
- [IP.SPP.4.5] Se registra toda la actividad
- [IP.SPP.4.7] Se realizan copias de seguridad periódicas de los registros de actividad
- [S.3.6.1] Se analizan las implicaciones para la continuidad del negocio
- [S.3.6.2] Se establece un protocolo de actuación en caso de contingencia
- [S.3.6.4] Los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales
- [AUX.AC.6] Alarma en tiempo real cuando el sistema se sale de especificaciones
- [L.7.2.1] La instalación contra incendios cumple la normativa industrial
- [L.7.2.9] Existe un plan de prevención de incendios (formación, concienciación, etc.)
- [H.IA.4.1] Se mantiene un registro de todos los usuarios con su identificador
- [H.IA.4.2.1] Altas: creación de nuevas cuentas
- [H.IA.4.2.2] Activación de cuentas de usuario
- [H.IA.4.2.3] Modificación de cuentas de usuario
- [H.IA.4.2.4] Suspensión temporal de cuentas de usuario
- [H.IA.4.2.5.2] Los identificadores no se reutilizan
- [H.IA.4.2.5.3] La información relevante se retiene de acuerdo a la normativa de seguridad

- [H.IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticador
- [H.IA.4.7] El usuario confirma la recepción del autenticador
- [H.IA.4.8] El usuario se hace cargo personalmente del control del autenticador
- [H.IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)
- [H.VM.4.2] daños sobre los activos del sistema
- [H.VM.4.3] perjuicios a terceros
- [H.VM.4.4] daños colaterales
- [H.VM.6.1] medidas cautelares
- [D.TS.1.1] Se tienen en cuenta los requisitos de no repudio
- [D.TS.1.3] Se definen roles y responsabilidades
- [D.TS.1.4] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos
- [D.TS.1.5] Se tienen en cuenta los requisitos de control: registro y auditoría
- [D.TS.1.7] Se tienen en cuenta los requisitos de interoperabilidad: actuales y previsiones futuras
- [S.1.2.1.2] Se tiene en cuenta el marco legal
- [S.1.2.1.3] Se tiene en cuenta la política interna
- [S.1.2.1.4] Se establecen límites al uso privado
- [COM.Internet.1.1] Se dispone de normativa sobre el uso de los servicios Internet
- [S.2.1.1] Se dispone de un registro de servicios internos
- [S.2.1.2] Se identifica el propietario (persona responsable)
- [S.2.1.3] El inventario se actualiza regularmente
- [S.CM.5.4] Se evalúa el impacto en los controles de monitorización
- [S.3.1.1] Se dispone de un registro de servicios subcontratados
- [S.3.1.3] Se identifican las aplicaciones sensibles o críticas que debe retener la Organización
- [S.3.1.4] Se identifican los riesgos derivados de depender de un proveedor externo
- [S.3.2.1] Se define la política aplicable sobre seguridad de la información
- [S.3.2.2] Constan las obligaciones de todas las partes
- [S.3.2.7] Se establecen los términos para la implicación de terceros (subcontratistas)
- [SW.4.2] Se dispone de los documentos que acreditan la propiedad
- [SW.4.3] Se dispone de un procedimiento para copias
- [SW.4.6] Se dispone de mecanismos de auditoría
- [SW.start.1] Se dispone de normativa de paso a operación / producción
- [SW.start.2] Se dispone de procedimientos de paso a operación / producción
- [SW.start.3] Se requiere autorización previa
- [SW.start.4] Se revisa la corrección y completitud de la documentación

- [SW.op.a.2.1] Se requiere autorización previa
- [HW.start.1] Se dispone de normativa de paso a operación / producción
- [HW.start.2] Se dispone de procedimientos de paso a operación / producción
- [HW.start.3] Se requiere autorización previa
- [HW.start.4] Se revisa la corrección y completitud de la documentación
- [HW.CM.5.2] Se evalúa el impacto en la confidencialidad de los datos
- [HW.CM.5.4] Se evalúa el impacto en los controles de monitorización
- [HW.PCD.a.1] Se dispone de un canal para reporte de incidentes
- [HW.PCD.a.3] Se dispone de procedimientos para gestión de incidentes
- [COM.cont.b] Las medios alternativos están sujetos a las mismas garantías de protección que los habituales
- [COM.cont.c] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento
- [COM.aut.1] Se requiere autorización previa
- [COM.CM.2.1] Se sigue un procedimiento formal de autorización de cambios
- [COM.CM.2.2] Se comunican los detalles del cambio a todo el personal afectado
- [MP.4.3.1] Se dispone de normativa para el transporte de soportes
- [MP.4.3.2] Se dispone de procedimientos para el transporte de soportes
- [MP.4.3.3.2] Se dispone de una relación de mensajeros autorizados por la Dirección
- [L.2.1] Se dispone de un registro de instalaciones propias
- [L.2.3] Se identifica al responsable en cada instalación
- [L.2.4] El inventario se actualiza regularmente
- [PS.4.1] Se dispone de un inventario de puestos de trabajo
- [H.IR.9.1] Se han establecido canales para la comunicación de las deficiencias
- [H.IR.e.3.1] Requisitos de seguridad
- [H.IR.e.3.2] Responsabilidades legales y contractuales
- [H.IR.e.3.3] Amenazas potenciales
- [H.IR.e.3.4] Vulnerabilidades identificadas
- [BC.5.1] Se dispone de un plan de gestión de crisis
- [G.exam.1] Se dispone de normativa de certificación, acreditación y revisiones de seguridad
- [G.exam.2] Se dispone de procedimientos de certificación, acreditación y revisiones de seguridad
- [NEW.S.2.1] Se tienen en cuenta los requisitos de control de acceso
- [NEW.S.2.2] Se tienen en cuenta los requisitos de identificación y autenticación
- [NEW.SW.1] Se establecen previamente los requisitos funcionales
- [NEW.SW.2.1] Se tienen en cuenta las obligaciones legales

- [NEW.SW.2.2] Se tienen en cuenta las obligaciones contractuales
- [NEW.SW.2.3] Se tienen en cuenta los estándares aplicables
- [NEW.SW.2.4] Se tiene en cuenta la política de seguridad de la organización
- [NEW.SW.2.5] Se tienen en cuenta requisitos futuros de certificación y/o acreditación
- [NEW.SW.4.1] Adquisición de SW solamente de fuentes reputables
- [NEW.HW.2.1] Se tienen en cuenta los requisitos de control de acceso
- [NEW.HW.2.2] Se tienen en cuenta los requisitos de identificación y autenticación
- [NEW.HW.2.5] Se tienen en cuenta los requisitos de confidencialidad
- [NEW.COM.2.1] Se tienen en cuenta los requisitos de control de acceso
- [NEW.COM.2.2] Se tienen en cuenta los requisitos de identificación y autenticación
- [NEW.COM.2.4] Se tienen en cuenta los requisitos de integridad
- [G.plan.1.1] Se monitoriza el uso de los recursos
- [G.plan.1.2] Se estiman las necesidades de procesamiento
- [G.plan.1.3] Se estiman las necesidades de software
- [G.plan.1.5] Se estiman las necesidades de almacenamiento
- [G.plan.1.6] Se estiman las necesidades de transmisión
- [G.plan.1.8] Se estiman las necesidades de concienciación y formación
- [HW.cont.5] Se monitorizan fallos e incidentes
- [HW.cont.6] Se registran los fallos, reales o sospechados y de mantenimiento preventivo y correctivo
- [D.2.1.1.4] Se siguen las directrices de clasificación definidas por leyes, reglamentos y acuerdos internacionales
- [COM.SC.7] Se activan los servicios de registro de actividad
- [S.2.9.1.4] ... de integridad
- [S.2.9.1.5] ... de registro
- [HW.cont.4] Se ejecutan regularmente las rutinas de diagnóstico
- [H.AC.8.1.2] Se revisan cuando hay cambios de puesto o de función
- [G.2.2.a] Se forma a los afectados
- [G.2.2.c] Se dispone de certificación independiente
- [H.AU.3.2.3] El sistema puede configurarse para retener todo el contenido relativo a una sesión de usuario
- [H.AC.2.2] Procedimiento de cancelación de privilegios
- [COM.op.4] Formación del personal en configuración de las comunicaciones
- [AUX.power.1] Se dimensiona el sistema considerando necesidades futuras
- [G.2.3.1] El acceso se limita a quien necesita conocer
- [NEW.COM.2.5] Se tienen en cuenta los requisitos de confidencialidad
- [H.VM.2.4] de las aplicaciones (SW)
- [S.CM.5.2] Se evalúa el impacto en la confidencialidad de los datos

- [NEW.S.2.5] Se tienen en cuenta los requisitos de confidencialidad
- [IP.SPP.3.3] Se revisa periódicamente el tráfico autorizado
- [H.IR.b.1] Tipo de incidente
- [H.IR.b.2] Momento en que se ha producido
- [H.IR.b.3] Persona que realiza la notificación
- [H.IR.b.4] A quién se le comunica
- [H.IR.b.5] Efectos derivados de la misma
- [H.IR.b.6] Acciones tomadas
- [D.2.3.2] Se dispone de los documentos que acreditan la propiedad
- [D.2.3.3] Se dispone de un procedimiento para copias
- [D.2.3.4] Se dispone de mecanismos de auditoría
- [S.CM.1] Se dispone de normativa de control de cambios
- [S.CM.3.1] Se sigue un procedimiento formal de autorización de cambios
- [S.CM.3.2] Se comunican los detalles del cambio a todo el personal afectado
- [S.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio
- [SW.backup.1.2] Procedimientos de restauración
- [SW.backup.1.3] Procedimientos de retención de copias de seguridad
- [SW.backup.1.4] Procedimientos de destrucción de copias de seguridad
- [SW.op.1] Se dispone de normativa relativa al software en producción
- [SW.CM.2.2] Se comunican los detalles del cambio a todo el personal afectado
- [SW.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio
- [HW.cont.b] Las medios alternativos están sujetos a las mismas garantías de protección que los habituales
- [HW.cont.c] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento
- [HW.op.1.1] Los nuevos medios deben tener la aprobación adecuada, autorizando su propósito y uso
- [HW.op.1.2] Se comprueba que son compatibles con los demás dispositivos del sistema
- [HW.op.1.3] Se requiere autorización previa para el uso de medios informáticos personales para el tratamiento de la información de la Organización
- [HW.CM.2.1] Se sigue un procedimiento formal de autorización de cambios
- [HW.CM.2.2] Se comunican los detalles del cambio a todo el personal afectado
- [HW.CM.a] Se planifica el cambio de forma que minimice la interrupción del servicio
- [HW.CM.f] Todos los cambios quedan registrados

- [HW.PCD.1] Se mantiene un inventario de equipos móviles con identificación del responsable de cada uno
- [HW.PCD.6] Se sigue un plan de concienciación sobre los riesgos y las medidas pertinentes
- [HW.PCD.7] Se sigue un plan de formación sobre las medidas pertinentes
- [HW.PCD.9.1] Normas y recomendaciones para su conexión a redes
- [HW.PCD.9.2] Normas y recomendaciones para su uso en lugares públicos
- [HW.PCD.9.3] Normas y recomendaciones para su almacenamiento cuando no se usa
- [COM.CM.1.2] Se han designado responsables para realizar cambios
- [COM.CM.1.3] Se han designado responsables para abortar y, en su caso recuperar, la situación inicial antes de un cambio
- [IP.1.1] Las conexiones requieren autorización previa
- [IP.1.2] Se dispone de un inventario de conexiones autorizadas
- [IP.1.4] Los usuarios y procesos autorizados a usar el enlace sólo disfrutan de los derechos mínimos imprescindibles
- [MP.4.1.6] Se requiere autorización previa antes de desprenderse de un soporte
- [MP.5.1] Se requiere autorización previa para sacar soportes de las instalaciones
- [MP.5.4] Se dispone de normativa de uso de soportes fuera de las instalaciones
- [MP.end.1] Se dispone de normativa que determina qué soportes deben ser destruidos de forma segura
- [MP.end.2] También se destruyen aquellos soportes de los que no puede eliminarse la información de forma segura
- [MP.end.3] Se dispone de procedimientos para la destrucción de soportes
- [H.IR.5.3.2] Daños sobre los activos del sistema
- [H.IR.5.3.3] Perjuicios a terceros
- [H.IR.5.3.4] Daños colaterales
- [H.IR.e.1] Concienciación en la detección y reporte de incidentes
- [G.1.2.1] Representación de todos los áreas de la organización
- [G.1.2.2] Se garantiza que todas las actividades de seguridad se llevan a cabo según la política
- [G.1.2.3] Se identifican no conformidades e incumplimientos
- [G.1.2.4] Se aprueban metodologías, procedimientos, normas, etc
- [G.1.4.1] Se identifican claramente los activos y los procesos de seguridad asociados con cada sistema específico
- [G.1.4.2] Se nombra al responsable de cada activo o proceso de seguridad
- [G.1.4.3] Se documentan los detalles de cada responsabilidad
- [G.1.4.4] Se definen y documentan claramente los niveles de autorización
- [G.1.5] Se dispone de asesoramiento especializado en seguridad

- [G.3.3.1] Emanan y están aprobadas por el responsable de seguridad
- [G.3.3.2] Se precisa lo que es uso adecuado y uso indebido
- [G.3.3.3] Se precisa la responsabilidad de las personas respecto de su cumplimiento y violación
- [G.3.3.4] Todo el personal de la organización tiene acceso a los documentos
- [G.3.3.6] Se revisan regularmente
- [G.3.5] Se revisa periódicamente el cumplimiento por parte del personal
- [G.exam.6.1] Regular (periodicidad establecida)
- [NEW.S.1.1] Se tienen en cuenta las obligaciones legales
- [NEW.S.1.2] Se tienen en cuenta las obligaciones contractuales
- [NEW.S.1.3] Se tienen en cuenta los estándares aplicables
- [NEW.S.1.4] Se tiene en cuenta la política de seguridad de la organización
- [NEW.S.1.5] Se tienen en cuenta requisitos futuros de certificación y/o acreditación
- [NEW.HW.1.1] Se tienen en cuenta las obligaciones legales
- [NEW.HW.1.2] Se tienen en cuenta las obligaciones contractuales
- [NEW.HW.1.3] Se tienen en cuenta los estándares aplicables
- [NEW.HW.1.4] Se tiene en cuenta la política de seguridad de la organización
- [NEW.HW.1.5] Se tienen en cuenta requisitos futuros de certificación y/o acreditación
- [NEW.COM.1.1] Se tienen en cuenta las obligaciones legales
- [NEW.COM.1.2] Se tienen en cuenta las obligaciones contractuales
- [NEW.COM.1.3] Se tienen en cuenta los estándares aplicables
- [NEW.COM.1.4] Se tiene en cuenta la política de seguridad de la organización
- [NEW.COM.1.5] Se tienen en cuenta requisitos futuros de certificación y/o acreditación
- [H.IR.2.1.3] Se dispone de normativa para la recogida de información sobre nuevos virus (listas de correos, consulta de páginas web, etc.)
- [IP.BS.2.7] Se activan los servicios de registro de actividad
- [NEW.SW.5.7.2] IPR: Se establecen acuerdos sobre licencia, propiedad del código y derechos de propiedad intelectual
- [MP.end.5] Se mantiene un registro de soportes destruidos
- [IP.BS.6] Se emplean productos certificados o acreditados
- [H.IA.1] Se dispone de normativa de identificación y autenticación
- [H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación
- [H.AC.a.6] Sólo se presenta la mínima información imprescindible durante el proceso de conexión
- [H.AC.a.7] Sólo se solicita la mínima información imprescindible para conectarse
- [H.AC.a.8] No se ofrecen mensajes de ayuda durante la conexión

- [H.AC.a.9] No se muestra identificación alguna del sistema o aplicación hasta que termina el proceso de conexión
- [H.AC.a.a] Se valida la información de conexión sólo tras rellenar todos los datos de entrada
- [H.tools.AV.a] Comprobación de virus desde diferentes puntos de la red
- [S.1.1] Se dispone de normativa relativa al uso de los servicios
- [S.1.2.a.1] Se designa el responsable para la administración del software
- [COM.wifi.1] Se requiere autorización previa para desplegar puntos de acceso (AP)
- [COM.wifi.3] Se requiere autorización previa para la conexión de clientes
- [PS.2.1] Se dispone de una relación de personal propio
- [PS.2.3] Se identifica el responsable
- [PS.2.4] Se revisa periódicamente
- [PS.6.2] Se actualizan los acuerdos de confidencialidad
- [H.IR.5.6.1] internos
- [H.IR.8.1] Hay canales establecidos para la comunicación de los incidentes
- [H.IR.8.2] Hay canales establecidos para dar respuesta a los incidentes
- [PS.8.1.2] spam
- [H.tools.TM.1] Se requiere autorización previa para su utilización
- [H.tools.TM.2] La herramienta se actualiza regularmente
- [H.tools.TM.3] Es posible recopilar, mostrar y analizar el tráfico de red así como de dividir las cabeceras y contenido del tráfico de red en los campos para una gran variedad de protocolos (ARP, RARP, ICMP, IGMP, TCP, UDP, FTP, Telnet, SMTP, DNS, HTTP, SNMP, SSL, IPX)
- [H.tools.TM.4] Permite crear y aplicar filtros de captura para establecer qué tipos de tráfico de red deben recopilarse
- [H.tools.TM.6] Es posible configurar reglas de autenticación y acceso
- [SW.SC.7] Se activan los servicios de registro de uso
- [S.start.2] Se revisa la corrección y completitud de la documentación
- [S.start.7] Los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales
- [S.start.8] Se ejecuta el plan de concienciación y formación en materia de seguridad
- [S.CM.2.2] Se han designado responsables para realizar cambios
- [S.CM.2.3] Se han designado responsables para abortar y, en su caso recuperar, la situación inicial antes de un cambio
- [S.2.9.2] Redacción y aprobación de un documento que consigne los términos acordados entre las partes
- [S.3.7.1] Se requiere autorización previa
- [S.3.7.3] Se planifica de forma que minimice la interrupción del servicio

- [S.3.7.6] Se actualizan todos los procedimientos de producción afectados
- [SW.CM.1.2] Se han designado responsables para realizar cambios
- [SW.CM.1.3] Se han designado responsables para abortar y, en su caso recuperar, la situación inicial antes de un cambio
- [SW.CM.h.2] Se actualiza la documentación del sistema
- [HW.op.4.1] Se requiere autorización previa para su utilización
- [HW.CM.1.2] Se han designado responsables para realizar cambios
- [HW.CM.1.3] Se han designado responsables para abortar y, en su caso recuperar, la situación inicial antes de un cambio
- [PS.4.5.1] ... de gestión de la propiedad intelectual (IPR)
- [G.1.1.2] Define claramente las funciones de seguridad
- [G.1.1.3] Aprueba las designaciones de responsables de seguridad
- [G.1.1.4] Identifica los objetivos de seguridad
- [G.1.1.5] Revisa, evalúa y aprueba la normativa de seguridad
- [G.1.1.6] Asegura la coordinación en materia de seguridad dentro de la organización
- [G.3.1.1] Se identifican los requisitos legales
- [G.3.1.2] Se identifican los requisitos reglamentarios (sectoriales)
- [G.3.1.3] Se identifican los requisitos contractuales
- [G.3.1.4] Se dispone de asesoría legal
- [G.3.1.5] Se han identificado los roles y responsabilidades requeridas
- [G.3.2.7] El documento se gestiona formalmente
- [NEW.SW.5.5.2] El entorno de pruebas simula realísticamente el entorno de producción
- [NEW.SW.5.5.4] Se revisa la corrección y completitud de la documentación
- [COM.CM.4.1] Se evalúa el impacto en la prestación de los servicios
- [S.3.3.c] Se forma a los administradores y usuarios en los métodos y procedimientos de seguridad
- [L.AC.c.1.3] Se identifica el responsable
- [G.1.3.3] Responsable de la seguridad de la información
- [G.3.2.3] Está aprobada y respaldada por la Dirección
- [D.2.4] Se dispone de normativa de retención de datos
- [NEW.SW.3.3] Se tienen en cuenta los requisitos de disponibilidad
- [S.3.5.3.4] Se usa un producto certificado o acreditado
- [L.7.2.4] Están debidamente señalizadas las vías de evacuación
- [L.7.2.7] Se revisan regularmente las áreas riesgo especial (cuarto de basuras, cuadros de alimentación, etc.)
- [L.7.2.8] Se revisan regularmente las instalaciones por los bomberos o personal especializado
- [L.7.2.e] Se ha identificado el personal para emergencias / intervención / evacuación
- [L.7.2.f] Se sigue un plan de mantenimiento y verificación de los dispositivos y los sistemas contra incendios
- [L.7.2.i] Se realizan regularmente simulacros internos

- [G.plan.1.9] Se estiman las necesidades de mobiliario y equipamiento de apoyo
- [HW.op.3.1] Se requiere autorización previa para el uso de equipos para tratamiento de información fuera de los locales de la Organización
- [HW.op.3.4] Se dispone de normativa de uso de equipos fuera de las instalaciones
- [G.2.2.1] Se revisa la documentación del sistema (nueva o actualizada)
- [G.2.2.2] Se revisan las medidas de seguridad a implantar
- [G.2.2.3] Se revisa la documentación de seguridad
- [G.2.2.4] Se revisan los procedimientos de operación del sistema
- [G.2.2.5] Se revisan los procedimientos de recuperación ante errores y de reinicio
- [G.2.2.6] Se comrpueba la facilidad de uso
- [G.2.2.7] Se comprueba el rendimiento y capacidad de procesamiento
- [G.2.2.8] Se estudian los efectos en el rendimiento y en la seguridad de su implantación
- [G.2.2.b] Los operadores y usuarios son consultados en el proceso de desarrollo
- [NEW.SW.5.3.2] Se nombra un responsable del código fuente para cada aplicación
- [NEW.SW.5.8.4] Existe una descripción de las herramientas de verificación
- [SW.4.1] Se dispone de normativa relativa al cumplimiento de los derechos
- [HW.2] Se dispone de normativa sobre el uso correcto de los equipos
- [S.3.5.3.2] Se protege el uso por medio de contraseña
- [IP.BS.4.1] Se explicita un responsable de la configuración
- [IP.BS.4.3.1] Consola local de configuración
- [AUX.AC.7] Mantenimiento: el sistema se revisa regularmente
- [S.2.9.1.3] ... de confidencialidad
- [D.2.3.1] Se dispone de normativa relativa al cumplimiento de los derechos
- [IP.SPP.7] Se ocultan las direcciones IP internas (servicio NAT o similar)
- [IP.SPP.8] Se ocultan los puertos internos (servicio PAT o similar)
- [NEW.HW.3.1] IPR: Se establecen acuerdos sobre los derechos de propiedad intelectual del producto
- [COM.cont.5] Se registran los fallos detectados, sean reales o sospechados
- [COM.cont.6] Se registran las actuaciones de mantenimiento preventivo y correctivo
- [COM.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio
- [NEW.S.2.3] Se tienen en cuenta los requisitos de disponibilidad
- [NEW.COM.2.3] Se tienen en cuenta los requisitos de disponibilidad

- [HW.CM.5.1] Se evalúa el impacto en la prestación de los servicios
- [NEW.HW.2.3] Se tienen en cuenta los requisitos de disponibilidad
- [AUX.wires.3] Se dispone de planos actualizados del cableado
- [H.tools.TM.5] Permite crear y aplicar filtros de presentación para establecer qué tipos de tráfico de red deben mostrarse
- [H.tools.TM.7] Es posible elaborar informes en diversos formatos (.html, .txt) y siguiendo diversos criterios (según el sistema, según la red, según la firma de producción)
- [S.3.1.2] Se requiere aprobación previa para el uso de servicios externos
- [S.3.2.6] Se contempla la protección de la información de carácter personal
- [IP.BS.1.3] Se realizan pruebas de regresión antes de instalar una nueva versión o parche
- [AUX.power.6.1] Actuación en caso de emergencia
- [AUX.power.6.2] El sistema se prueba regularmente
- [AUX.power.6.3] Mantenimiento: el sistema se revisa regularmente
- [L.AC.c.1.1] Se mantiene un registro de las llaves
- [L.AC.c.1.2] Se mantiene un registro de combinaciones de acceso
- [L.AC.c.1.4] El inventario se actualiza regularmente
- [PS.5.2.5.2] Procedimiento sancionador
- [SW.CM.h.3] Se destruye o se archiva la documentación anterior
- [G.3.2.2] Recoge los objetivos y la misión de la Organización
- [G.3.2.6] Incluye referencias normativas y procedimientos específicos
- [IP.SPP.3.1] El tráfico permitido requiere autorización previa
- [NEW.SW.5.8.3] Existe una descripción de las herramientas de desarrollo
- [HW.CM.j] Se actualizan todos los procedimientos de recuperación afectados
- [SW.CM.j] Se actualizan todos los procedimientos de recuperación afectados
- [S.3.2.3.1] Se establecen lo niveles de servicio deseados y los inaceptables
- [G.1.3.4] Responsable del sistema
- [G.3.2.1] Está coordinada con la Política de Seguridad Global de la Organización
- [G.3.2.4] Todo el personal de la organización tiene acceso al documento
- [S.3.7.2] Se estudia el impacto en el negocio
- [S.3.7.7] Se actualizan todos los procedimientos de recuperación afectados
- [G.2.3.3.1] Garantías de disponibilidad
- [G.2.3.5] Norma de copias de seguridad (backup)
- [S.2.9.1.1] ... de disponibilidad
- [S.CM.5.1] Se evalúa el impacto en la prestación de los servicios

Annex VII – Informe Anàlisi de Riscos PILAR

Informe extret de l'eina PILAR

Análisis de Riesgos

[2700AJFITA] 2700-Aj_FitaAlta 26.4.2016

Introducción

Código: 2700AJFITA
Nombre: 2700-Aj_FitaAlta

Descripción:

Anàlisi de riscos seguint la metodologia MAGERIT utilitzant l'aplicació micro Pilar per al treball de fi de Màster de la UOC amb l'organització fictícia "Ajuntament de Fita Alta"

Datos administrativos:

- desc: Anàlisi de Riscos de l'Ajuntament de Fita Alta -
- resp: Andreu Retamero Pallarès
- org: Ajuntament de Fita Alta
- ver: 1.0
- date: 12/04/2016

Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

Valoración del sistema

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

essential

activo	[D]	[I]	[C]	[A]	[T]
[IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
[NOT-ELEC] Notificacions telemàtiques	[1](1)	[4]	[4]	[4]	[4]
[POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]
[CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
[INFOPUB] Informació pública	[1](2)	[4](3)	[0](4)	[4]	[0]
[LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]
[TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
[CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
[VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4](5)

(1) [1.da] Pudiera causar la interrupción de actividades propias de la Organización

(2) Informació publica: calendari contribuent, ordenances, extractes dels acords de la JG, reglaments.. La no disponibilitat d'aquesta informació no suposa cap interrupció de servei, ni afecta a la productivitat i es pot obtenir per un altre canal (presencial o telefònic)

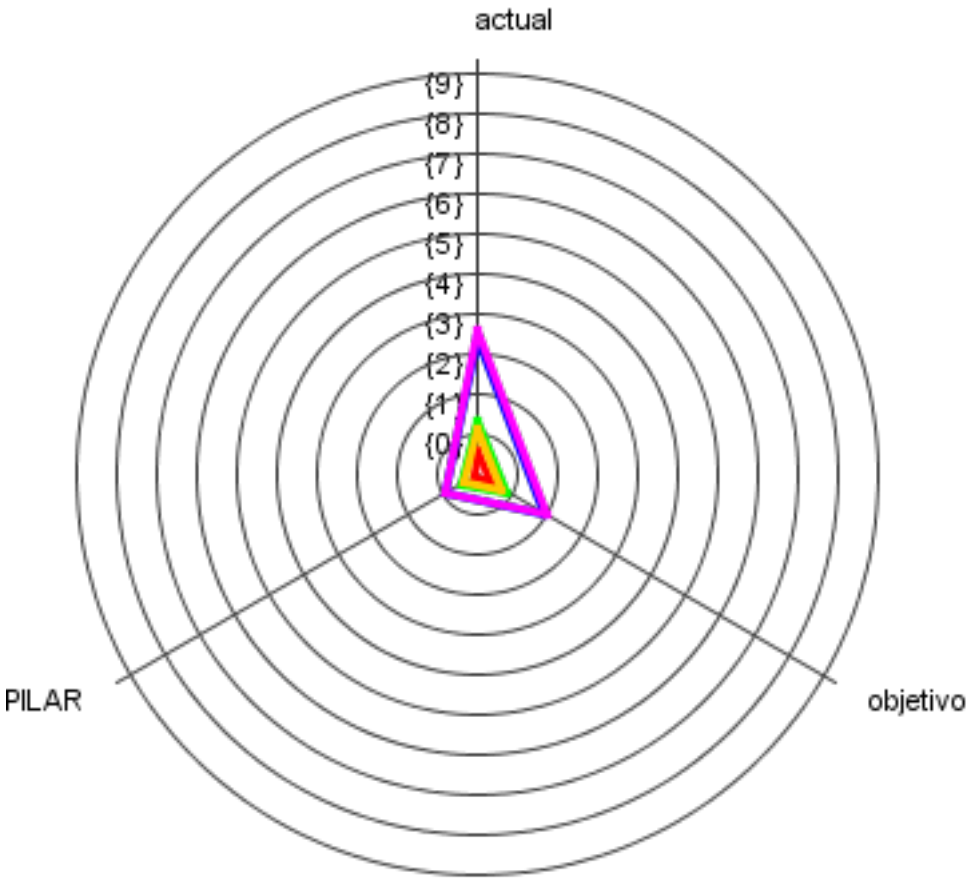
(3) La manipulació de la informació pública no causaria pèrdues econòmiques però si danys en la imatge de l'ajuntament davant tercers.
[b] por afectar gravemente a las relaciones con el público en general

(4) La informació és pública

(5) [cei] Intereses Comerciales / Económicos:

Riesgo sobre los activos esenciales

[INFOPUB] Informació pública

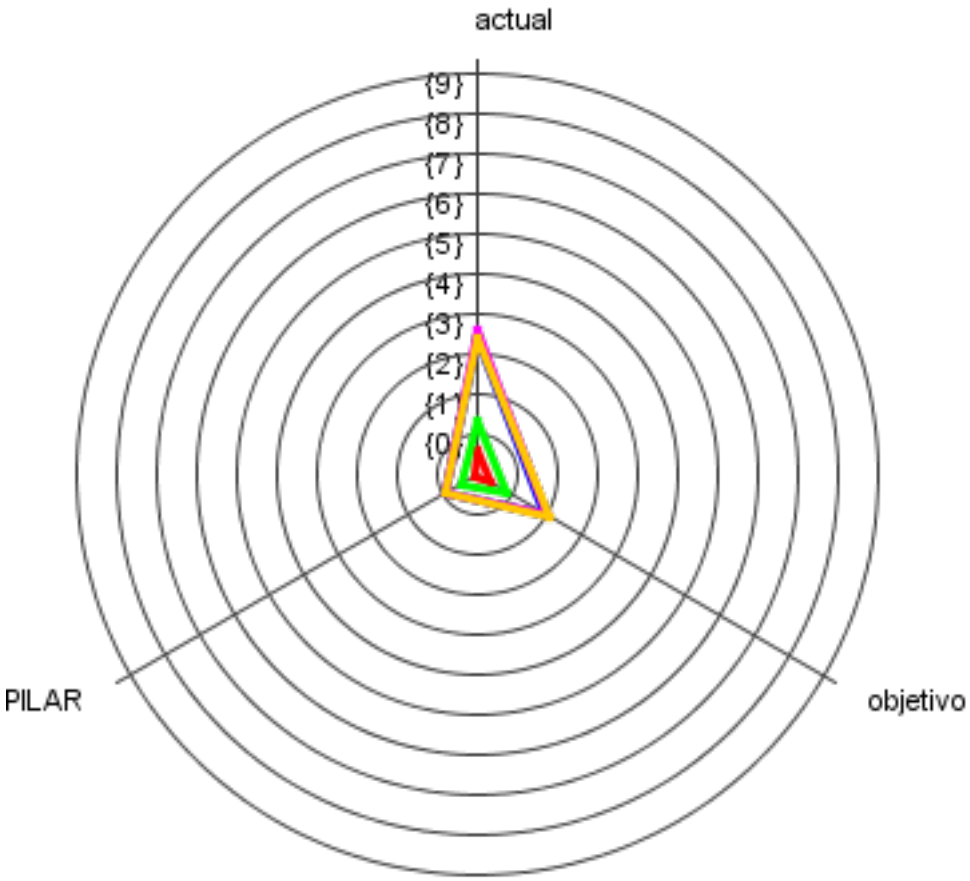


- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

[INFOPUB] Informació pública

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{1,3}	{3,6}	{1,1}
objetivo	{0,40}	{1,9}	{0,84}	{2,0}	{0,74}
PILAR	{0,09}	{0,86}	{0,45}	{0,84}	{0,38}

[TEE] Tauler Edictes Electrònic

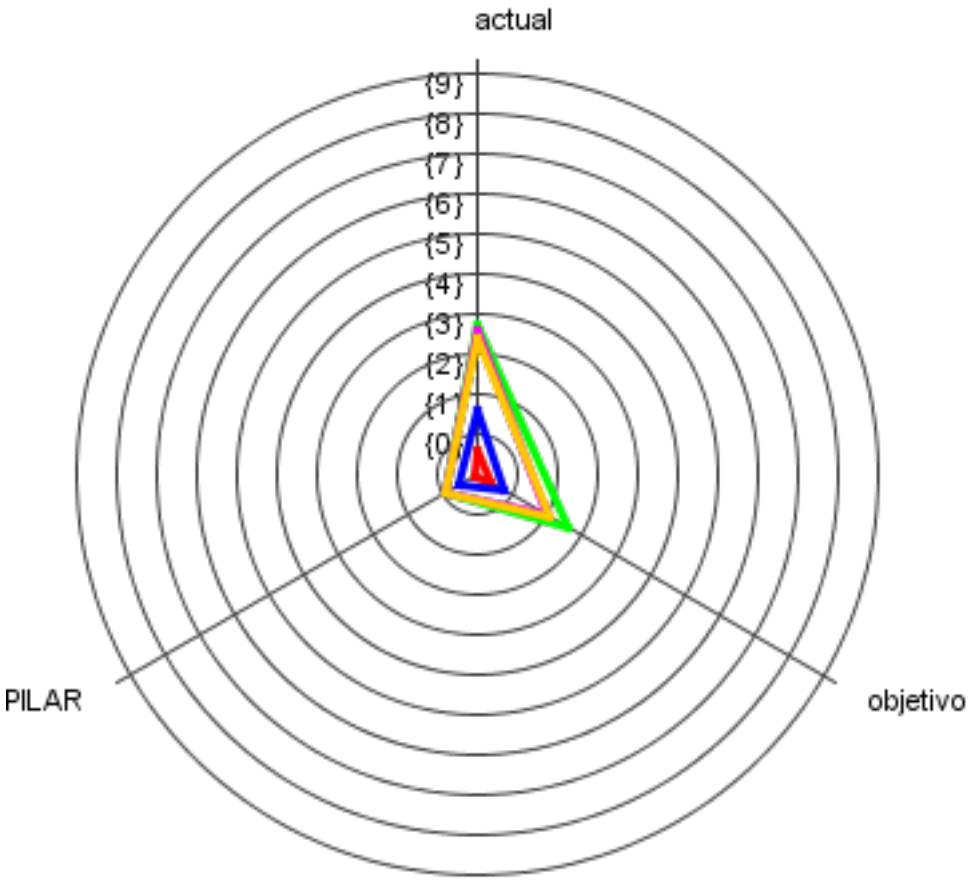


- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

[TEE] Tauler Edictes Electrònic

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{1,3}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{0,84}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,45}	{0,84}	{0,85}

[IniTram] Inici de tràmits

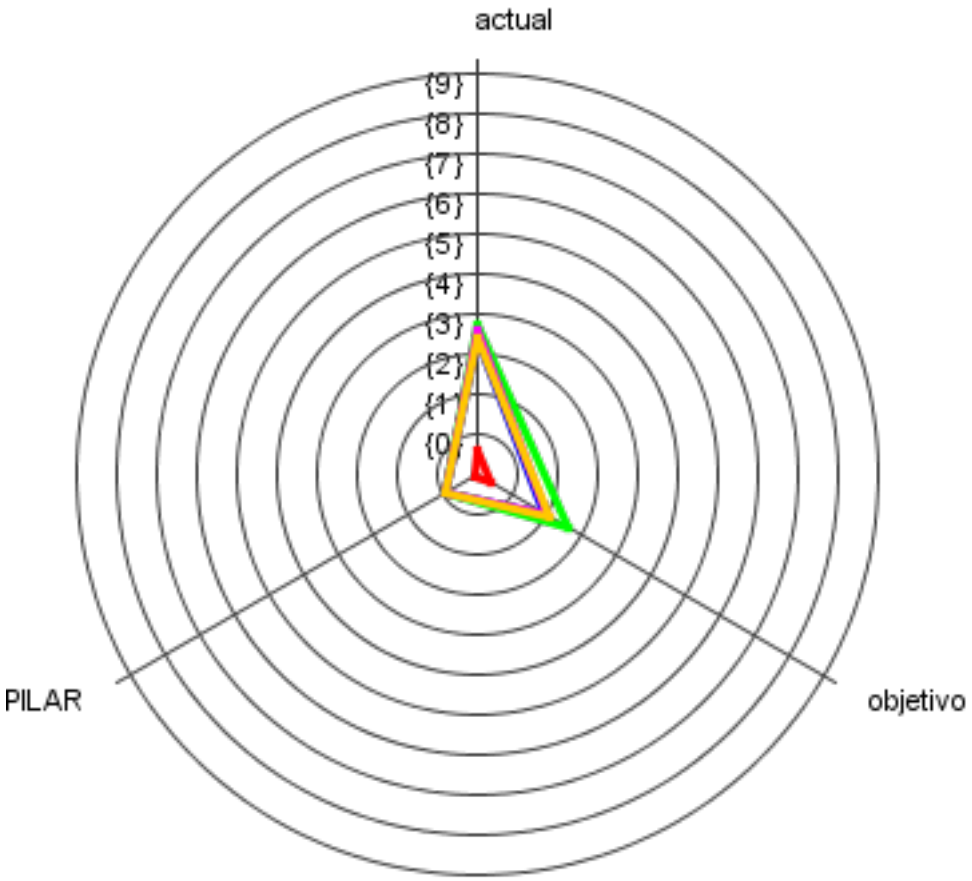


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[IniTram] Inici de tràmits

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{1,6}	{3,7}	{3,6}	{3,4}
objetivo	{0,40}	{0,82}	{2,6}	{2,0}	{2,1}
PILAR	{0,09}	{0,51}	{0,92}	{0,84}	{0,85}

[CARCIUTADANA] Carpeta ciutadana

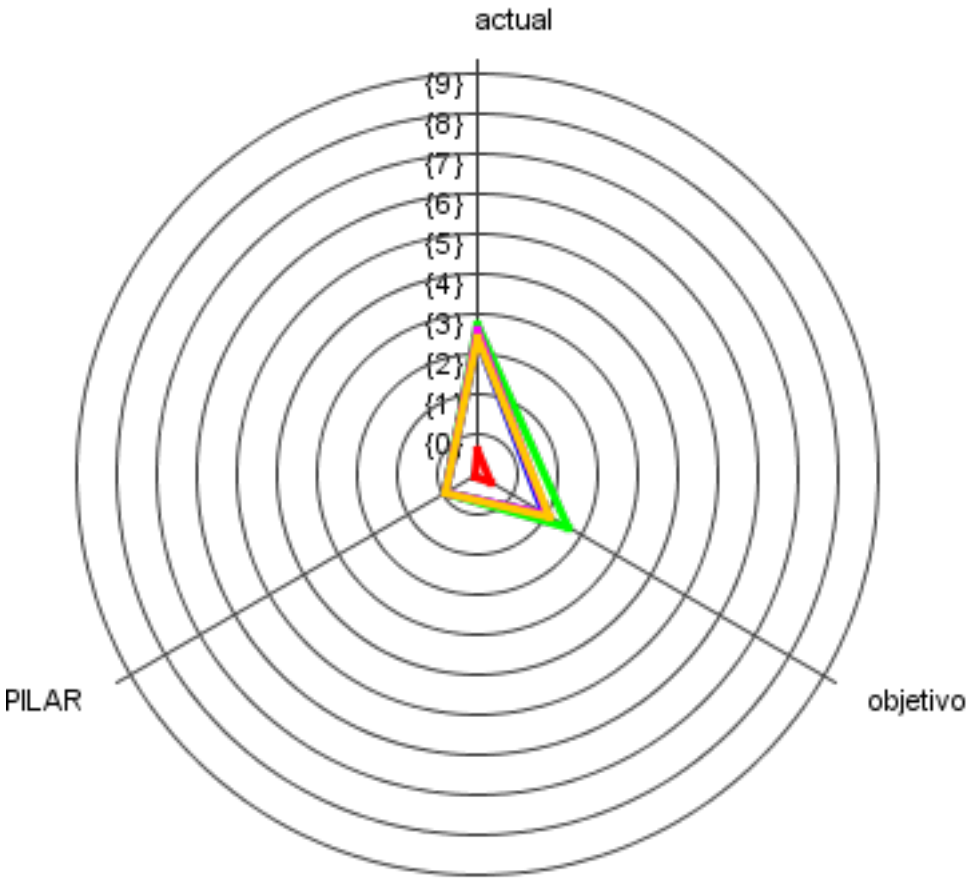


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[CARCIUTADANA] Carpeta ciutadana

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}

[CARPROVEIDOR] Carpeta del proveïdor

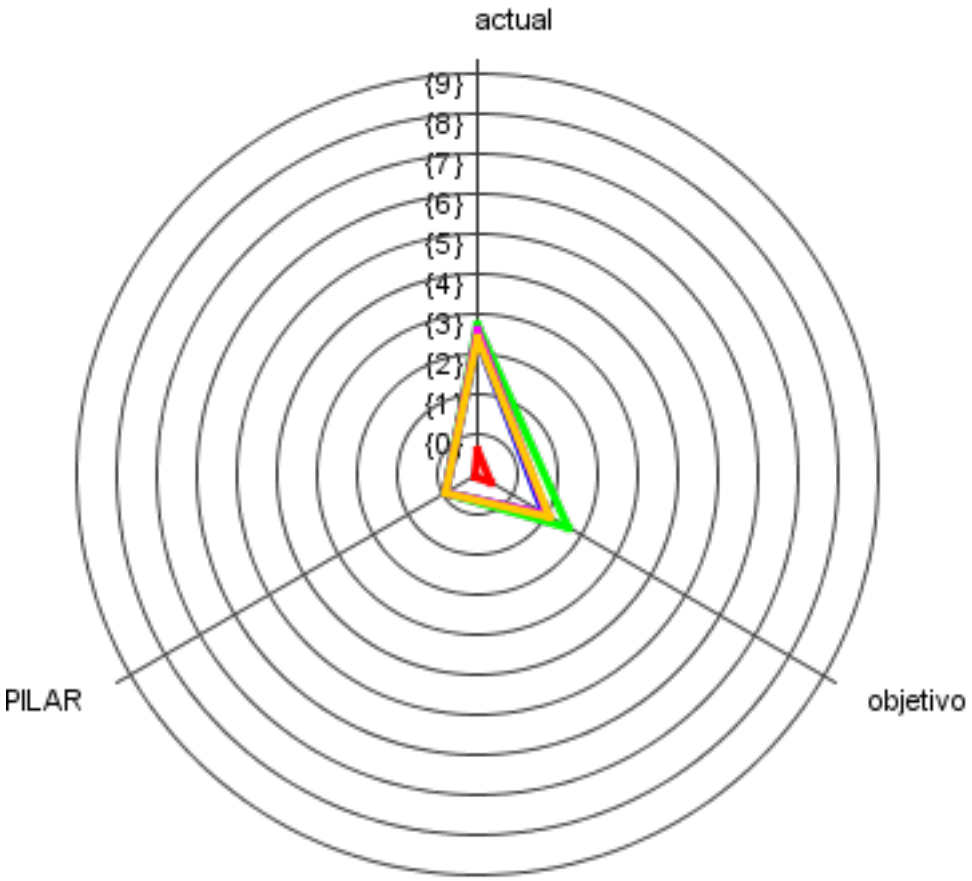


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[CARPROVEIDOR] Carpeta del proveïdor

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}

[VALDOCS] Validador de documents

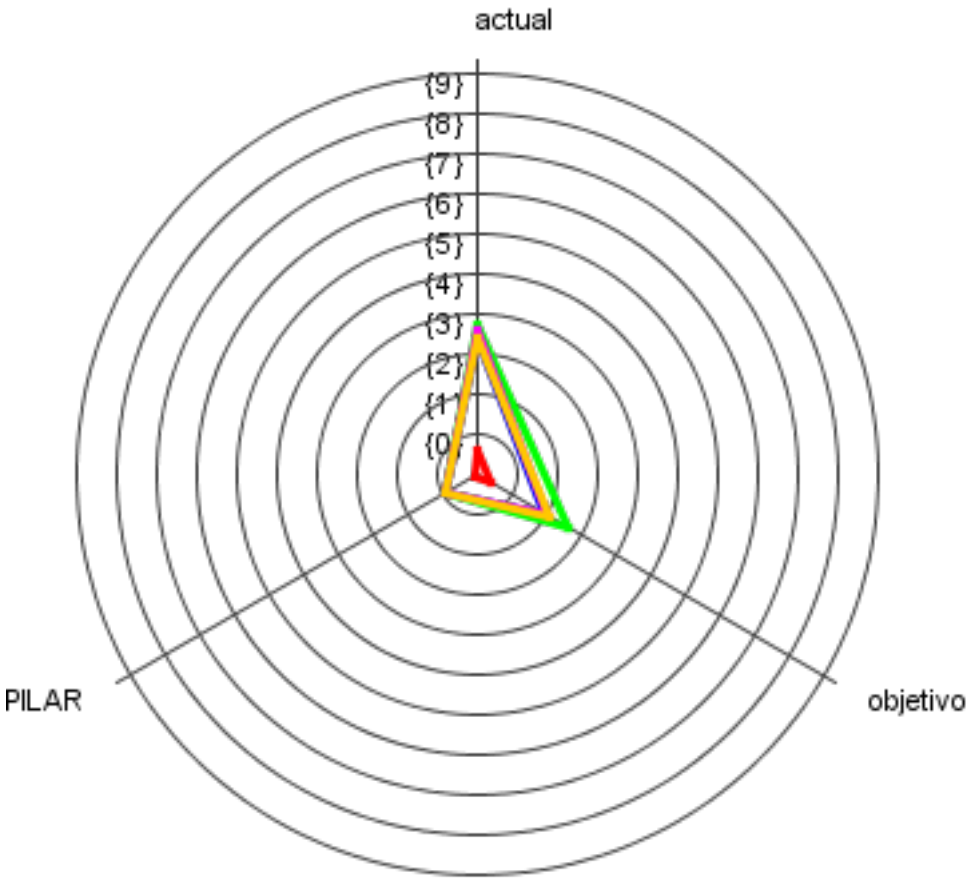


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[VALDOCS] Validador de documents

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}

[NOT-ELEC] Notificacions telemàtiques

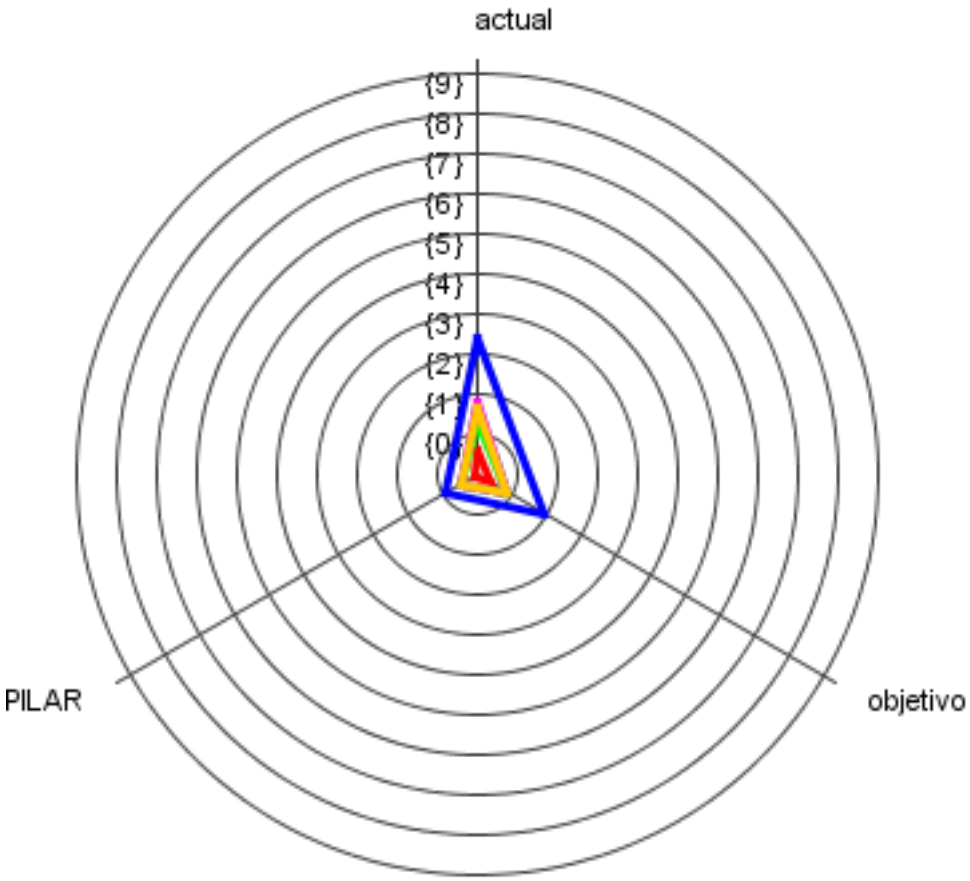


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[NOT-ELEC] Notificacions telemàtiques

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
objetivo	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
PILAR	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}

[LICIT] Licitacions

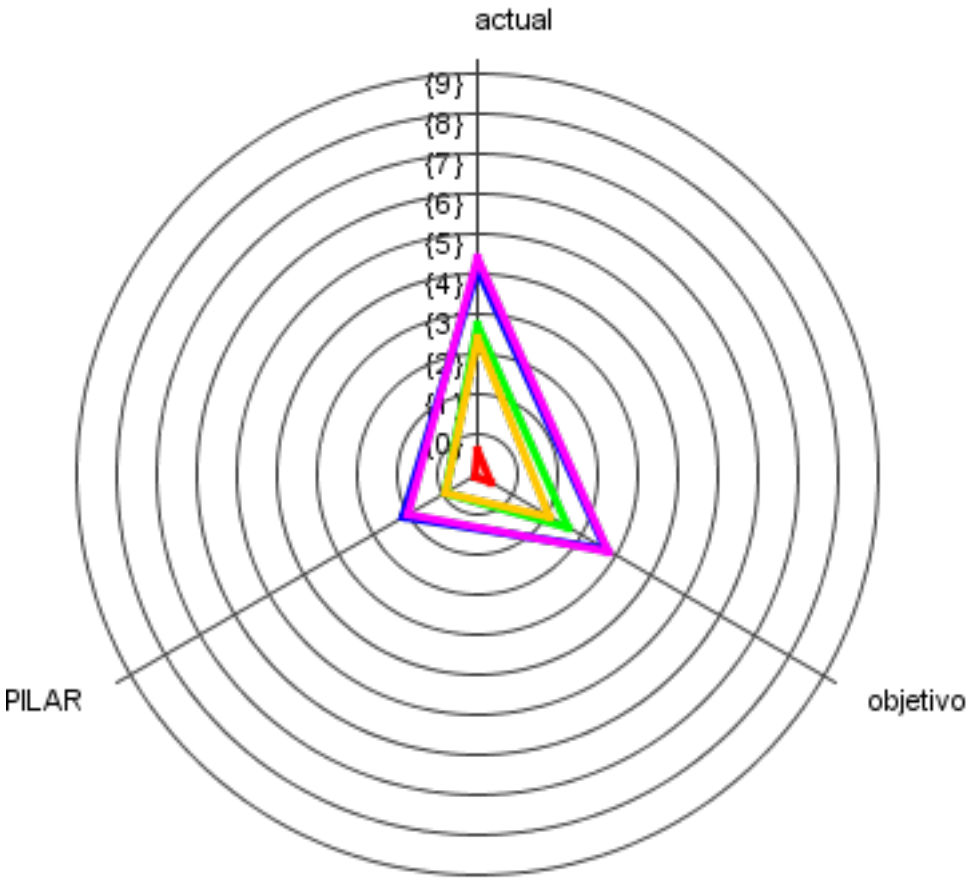


[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

[LICIT] Licitacions

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{3,4}	{1,3}	{1,8}	{1,7}
objetivo	{0,40}	{1,9}	{0,84}	{0,85}	{0,85}
PILAR	{0,09}	{0,86}	{0,45}	{0,48}	{0,49}

[POL] Pagaments On-Line



[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

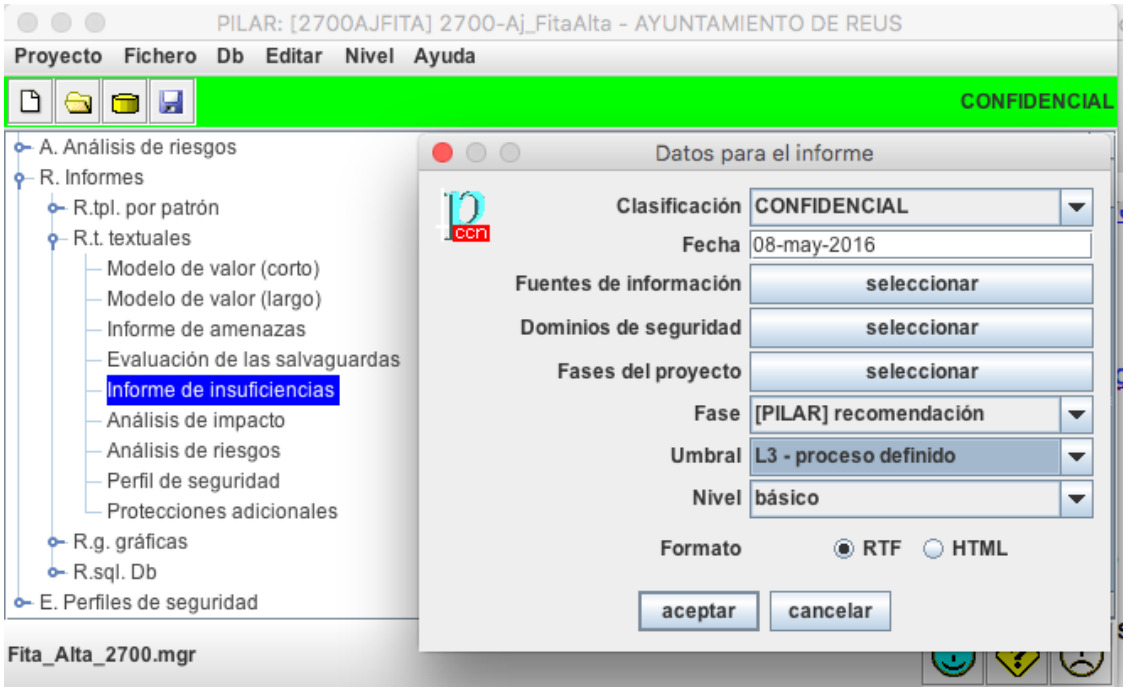
[POL] Pagaments On-Line

fase	[D]	[I]	[C]	[A]	[T]
actual	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}
objetivo	{0,40}	{3,7}	{2,6}	{3,8}	{2,1}
PILAR	{0,09}	{2,1}	{0,92}	{2,0}	{0,85}

Annex VIII – Informe insuficiències PILAR

L'informe d'insuficiències està extret dels informes subministrats per l'eina PILAR i ha estat generat amb els paràmetres següents:

- Fase de referència : [PILAR] Recomanació per a la norma ISO 27002:2013
- Llindar : Salvaguardes amb un nivell d'eficàcia inferior a "L3–Procés definit"
- Nivell de detall : Bàsic (Nivell de detall del llistat)



Informe de insuficiencias (vulnerabilidades)
proyecto: [2700AJFITA] 2700-Aj_FitaAlta
phase: [PILAR] recomendación

Relación de salvaguardas que adolecen de un nivel de eficacia inferior a "L3 - proceso definido".

Datos del proyecto

2700AJFITA	2700-Aj_FitaAlta
desc	Anàlisi de Riscos de l'Ajuntament de Fita Alta -
resp	Andreu Retamero Pallarès
org	Ajuntament de Fita Alta
ver	1.1
date	06/05/2016
biblioteca	[std] Biblioteca INFOSEC (8.11.2013)

Descripción

Anàlisi de riscos seguint la metodologia MAGERIT utilitzant l'aplicació micro Pilar per al treball de fi de Màster de la UOC amb l'organització fictícia "Ajuntament de Fita Alta"

Licencia

AJUNTAMENT DE FITA ALTA

niveles de madurez

5.17 L0 - inexistente
5.18 L1 - inicial / ad hoc
5.19 L2 - reproducible, pero intuitivo
5.20 L3 - proceso definido
5.21 L4 - gestionado y medible
5.22 L5 - optimizado

Dominios de seguridad

5.23 [base] Base

Fases del proyecto

5.24 [actual] situación actual
5.25 [objetivo] situación objetivo
5.26 [PILAR] recomendación

Dominio de seguridad: [base] Base

[H] Protecciones Generales

salvaguarda	A	R	[actual]	[objetivo]	[PILAR]
[H.IA] Identificación y autenticación	G	7	_-L3	_-L4	L2-L4
[H.IA.1] Se dispone de normativa de identificación y autenticación	G	3	L2	L3	L3
[H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación	G	3	L2	L3	L3
[H.IA.3] Identificación de los usuarios	G	5	L2-L3	L3	L3
[H.IA.4] Gestión de la identificación y autenticación de usuario	G	5	L0-L2	L2-L3	L2-L3
[H.IA.4.1] Se mantiene un registro de todos los usuarios con su identificador	G	2	L2	L2	L2
[H.IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario	G	5	L2	L2-L3	L2-L3
[H.IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador	G	4	L1	L3	L3
[H.IA.4.4] Se limita el número de autenticadores	G	3	L2	L3	L3

necesarios por usuario					
[H.IA.4.5] Los autenticadores se distribuyen de forma segura	G	3	L1	L3	L3
[H.IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticador	G	2	L0	L2	L2
[H.IA.4.7] El usuario confirma la recepción del autenticador	G	2	L1	L2	L2
[H.IA.4.8] El usuario se hace cargo personalmente del control del autenticador	G	2	L1	L2	L2
[H.IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)	G	2	L2	L2	L2
[H.IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello	G	5	L2	L3	L3
[H.IA.5] Cuentas especiales (administración)	G	5	L0-L3	L2-L3	L2-L3
[H.IA.7] {xor} Factores de autenticación que se requieren:	G	7	L2	L4	L3-L4
[H.IA.7.1] Algo que se tiene - token físico (ej. tarjeta)	G	7 (u)			L3-L4
[H.IA.7.1.1] Token físico - algo que se tiene	G	7			L3-L4
[H.IA.7.1.1.1] El usuario asume la responsabilidad de la custodia del token	G	4			L3
[H.IA.7.3] Certificados software (criptografía de clave pública)	G	7	L2-L3	L3	L3-L4
[H.IA.7.3.1] Se protege el uso por medio de contraseña	G	4	L2	L3	L3
[H.IA.7.3.3] Se usa un producto certificado o acreditado	G	4	L3	L3	L3
[H.IA.7.3.4] Se emplean algoritmos certificados / acreditados	T	4	L3	L3	L3
[H.IA.7.3.5] Se emplean parámetros certificados / acreditados	T	4	L3	L3	L3
[H.IA.7.4] Algo que se es - biometría (ej. huella dactilar)	G	7	L3	L3	L3-L4
[H.IA.7.4.3] Se emplea un producto certificado o acreditado	G	4	L3	L3	L3
[H.AC] Control de acceso lógico	T	8	_-L3	_-L3	L2-L5
[H.AC.1] Se dispone de normativa para el control de accesos	T	4	L2	L3	L3
[H.AC.2] Se dispone de procedimientos para las tareas de control de accesos	T	4	L1-L2	L2-L3	L2-L3
[H.AC.3] Se definen y documentan las autorizaciones de acceso	G	4	L1	L2	L3
[H.AC.4] Restricción de acceso a la información	T	5	L2	L3	L3
[H.AC.5] Se restringe el uso de las utilidades del sistema	T	5	L0-L2	L1-L3	L3
[H.AC.6] Se restringe el acceso a la configuración del sistema	T	6	L1-L3	L2-L3	L3-L4
[H.AC.7] Se controla el trabajo fuera del horario normal	T	5			L3

[H.AC.8] Gestión de privilegios	T	5	L0-L2	L1-L3	L2-L3
[H.AC.8.1] Se identifican los perfiles de acceso y sus privilegios asociados	T	2	L2	L2	L2
[H.AC.8.2] En la asignación de privilegios se tiene en cuenta el principio de 'privilegio mínimo necesario para realizar las tareas asignadas'	T	3	L2	L3	L3
[H.AC.8.3] En la asignación de privilegios se tiene en cuenta el principio de 'necesidad de conocer'	T	3	L2	L3	L3
[H.AC.8.4] Los derechos de acceso son aprobados por el propietario del servicio o de la información	T	2	L2	L2	L2
[H.AC.8.5] La comunicación de sus derechos a los usuarios consta por escrito	T	2	L1	L2	L2
[H.AC.8.6] Los usuarios reconocen por escrito que conocen y aceptan sus derechos	T	2	L2	L2	L2
[H.AC.8.7] Se separan las responsabilidades de administración y operación	T	4	L0	L1	L3
[H.AC.8.8] Se mantiene un registro de los privilegios de acceso	T	2	L0	L1	L2
[H.AC.8.9] El sistema mantiene los privilegios asociados a cada usuario	T	3	L2	L2	L3
[H.AC.8.a] Los privilegios se anulan cuando termina la autorización	T	5	L1	L2	L3
[H.AC.8.b] Los privilegios se revisan cuando el usuario cambia de responsabilidades o de función	T	5	L2	L3	L3
[H.AC.8.c] Los privilegios se anulan cuando el usuario abandona la organización	T	5	L2	L3	L3
[H.AC.9] Revisión de los derechos de acceso de los usuarios	T	5	L0-L2	L2-L3	L3
[H.AC.b] Conexión en terminales (logon)	T	6	L0-L3	L2-L3	L3-L4
[H.AC.b.2] Tras un intento fallido existe un retardo hasta que el siguiente intento sea posible	T	5	L1	L2	L3
[H.AC.b.3] Se bloquea la cuenta tras un número limitado de intentos fallidos	T	5	L3	L3	L3
[H.AC.b.4] Se requiere autorización para restablecer una cuenta bloqueada	T	5	L3	L3	L3
[H.AC.b.5] Se limita el tiempo permitido para efectuar el proceso de conexión	T	5	L0	L2	L3
[H.AC.b.6] Sólo se presenta la mínima información imprescindible durante el proceso de conexión	T	3	L3	L3	L3
[H.AC.b.7] Sólo se solicita la mínima información imprescindible para conectarse	T	3	L3	L3	L3
[H.AC.b.8] No se ofrecen mensajes de ayuda durante la conexión	T	3	L3	L3	L3
[H.AC.b.9] No se muestra identificación alguna del sistema o aplicación hasta que termina el proceso de conexión	T	3	L3	L3	L3
[H.AC.b.a] Se valida la información de conexión sólo tras rellenar todos los datos de entrada	T	3	L3	L3	L3
[H.AC.b.b] Se presenta un mensaje indicando el uso	T	3	L0	L2	L3

debido del sistema					
[H.AC.b.c] Se presenta un mensaje indicando que queda prohibido todo uso no autorizado	T	3	L0	L2	L3
[H.AC.b.d] Se presenta un mensaje indicando que toda la actividad podrá ser supervisada	T	3	L0	L2	L3
[H.AC.b.e] Tras la conexión, se muestra la fecha y hora de la anterior conexión realizada con éxito	T	3	L0	L2	L3
[H.AC.b.f] Tras la conexión, se muestran los intentos fallidos	T	3	L0	L2	L3
[H.AC.b.g] Las contraseñas no pueden ser almacenadas en ningún proceso automático (macros, teclas de función, etc.)	T	5	L3	L3	L3
[H.AC.c] Se limita el tiempo de conexión	T	5	L0-L3	L2-L3	L3
[H.AC.d] Se limita el número de sesiones concurrentes de un usuario	T	5			L3
[H.AC.e] Equipo informático de usuario desatendido	T	8	L1-L3	L2-L3	L3-L5
[H.AC.e.1] Concienciación de los usuarios	T	5	L1	L2	L3
[H.tools] Herramientas de seguridad	T	7	_-L3	_-L3	L2-L4
[H.tools.AV] Herramienta contra código dañino	T	7	L0-L3	L2-L3	L3-L4
[H.tools.AV.1] El programa se actualiza regularmente	T	4	L3	L3	L3
[H.tools.AV.3] Se revisan los programas y servicios de arranque del sistema	T	4	L2	L3	L3
[H.tools.AV.4] Se revisa cada aplicación cuando arranca	T	4	L1	L2	L3
[H.tools.AV.5] Se revisan los anexos al correo electrónico	T	5	L3	L3	L3
[H.tools.AV.6] Se revisa el contenido de las páginas web que se visitan	T	4	L2	L2	L3
[H.tools.AV.7] Se revisan todos los ficheros descargados	T	4	L3	L3	L3
[H.tools.AV.8] Se revisan los ficheros recibidos en un medio removible	T	4	L0	L2	L3
[H.tools.AV.9] Se revisan medios removibles cuando se conectan al sistema de información	T	4	L3	L3	L3
[H.tools.AV.a] Comprobación de virus desde diferentes puntos de la red	T	3	L3	L3	L3
[H.tools.AV.b] Se emplea un producto certificado o acreditado	T	5	L3	L3	L3
[H.tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión	T	6			L2-L4
[H.tools.CC] Herramienta de chequeo de configuración	T	6			L3-L4
[H.tools.TM] Herramienta de monitorización de tráfico	T	5	L2	L3	L2-L3
[H.tools.DLP] DLP: Herramienta de monitorización de contenidos	T	4	L0	L1	L2-L3
[H.tools.HP] Honey net / honey pot	T	5			L2-L3
[H.tools.SFV] Verificación de las funciones de seguridad	T	5			L3
[H.VM] Gestión de vulnerabilidades	G	6	L0-L3	L0-L3	L2-L4
[H.VM.1] Se dispone de personas dedicadas a la gestión	G	3	L1	L2	L3

de vulnerabilidades					
[H.VM.2] Se han previsto mecanismos para estar informados de vulnerabilidades ...	G	4	L1-L2	L1-L3	L2-L3
[H.tools.VA] Herramienta de análisis de vulnerabilidades	T	6	L1	L2	L3-L4
[H.VM.4] Se analiza el impacto potencial (estimación de riesgos)	G	3	L2	L2	L2-L3
[H.VM.5] Pruebas de penetración	G	4	L0-L3	L0-L3	L3
[H.VM.5.1] Las pruebas de penetración se aplican a los controles de seguridad física	G	4	L0	L0	L3
[H.VM.5.2] Las pruebas de penetración se aplican a los controles de seguridad lógica	G	4	L2	L2	L3
[H.VM.5.3] Se prueba desde Internet (atacantes externos)	G	4	L2	L3	L3
[H.VM.5.4] Se prueba a través de accesos WiFi	G	4	L0	L2	L3
[H.VM.5.5] Se prueba desde dentro (atacantes internos)	G	4	L1	L2	L3
[H.VM.5.6] Se realizan pruebas a nivel de red (network testing)	G	4	L0	L2	L3
[H.VM.5.7] Se realizan pruebas a nivel de aplicaciones	G	4	L2	L3	L3
[H.VM.5.8] Se incluyen pruebas de picaresca (social engineering)	G	4	L0	L2	L3
[H.VM.5.9] Se realiza un análisis previo basado en el conocimiento exhaustivo del sistema	G	4	L0	L2	L3
[H.VM.5.a] Se identifican las vulnerabilidades potenciales a partir del análisis previo	G	4	L2	L3	L3
[H.VM.5.b] Se realizan pruebas para determinar explotabilidad de vulnerabilidades identificadas	G	4	L1	L2	L3
[H.VM.5.c] Las pruebas se repiten regularmente	G	4	L3	L3	L3
[H.VM.5.d] Se realizan pruebas cuando se actualiza el software de base	G	4	L0	L1	L3
[H.VM.5.e] Se realizan pruebas cuando se despliegan nuevos servidores y servicios www	G	4	L0	L1	L3
[H.VM.5.f] Se realizan pruebas cuando se conecta el sistema a nuevas redes	G	4	L0	L1	L3
[H.VM.6] Se dispone de procedimientos de reacción	G	3	L1-L2	L2	L2-L3
[H.VM.7] Actuaciones	G	5	L2-L3	L3	L3
[H.VM.7.1] Se reparan urgentemente las vulnerabilidades que implican un alto riesgo	G	5	L3	L3	L3
[H.VM.7.2] Se reparan con diligencia las vulnerabilidades que implican un cierto riesgo	G	4	L2	L3	L3
[H.VM.7.3] Se planifica la reparación de las vulnerabilidades que implican un riesgo bajo	G	3	L2	L3	L3
[H.AU] Registro y auditoría	T	6	_-L3	_-L3	L2-L4
[H.AU.1] Administración	T	4	_-L1	_-L2	L3
[H.AU.1.1] Se dispone de normativa acerca del registro y la auditoría	T	4	L1	L2	L3
[H.AU.1.2] Se dispone de procedimientos para las	T	4			L3

tareas de auditoría y registro de actividad					
[H.AU.1.3] Gestión de las actividades de registro y auditoría	T	4	L0	L2	L3
[H.AU.1.4] Se dispone de un inventario de las fuentes de información	T	4			L3
[H.AU.1.5] Los eventos a registrar se incluyen en la documentación de seguridad del sistema	T	4			L3
[H.AU.2] Herramientas	T	6	_-L3	_-L3	L2-L4
[H.tools.LA] Herramienta para análisis de logs	T	4			L2-L3
[H.AU.2.2] Protección de las herramientas de auditoría de sistemas	T	3	L0	L2	L3
[H.AU.2.3] Prevención del mal uso de los mecanismos de registro de actividad	T	3			L2-L3
[H.AU.2.4] Sincronización de relojes	T	6	L1-L3	L2-L3	L3-L4
[H.AU.3] Información	T	5	L0-L3	L1-L3	L2-L3
[H.AU.4] Actividades	T	5	_-L3	_-L3	L3
[H.AU.4.1] Respuestas automáticas	T	3			L3
[H.AU.4.1.1] Generación de alarmas en tiempo real	T	3			L3
[H.AU.4.1.2] Terminación de procesos problemáticos	T	3			L3
[H.AU.4.1.3] Detención de servicios problemáticos	T	3			L3
[H.AU.4.1.4] Desconexión de usuarios sospechosos	T	3			L3
[H.AU.4.1.5] Inhabilitación de cuentas sospechosas	T	3			L3
[H.AU.4.2] Revisión de los registros	T	4	L0-L3	L1-L3	L3
[H.AU.4.3] Consolidación y reporte	T	5	L1	L2	L3
[H.AU.4.4] Destrucción de los registros	T	4			L3
[H.AU.4.5] Se gestionan los incidentes en las actividades de auditoría y registro	T	4			L3

[D] Protección de la Información

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[D.2] Se dispone de un inventario de activos de información	G	3	L0-L1	L2	L3
[D.3] Normativa	G	4	L0-L2	L1-L3	L2-L3
[D.3.1] Se clasifica la información	G	4	L0-L2	L1-L2	L2-L3
[D.3.2] Atributos de seguridad	G	2	L0	L1	L2
[D.3.2.1] El sistema mantiene los atributos de seguridad íntimamente ligados a la información almacenada, en proceso y transmitida	G	2	L0	L1	L2
[D.3.2.2] Los atributos de seguridad se mantienen asociados a la información cuando ésta se intercambia con otros sistemas	G	2	L0	L1	L2
[D.3.3] IPR: Se protegen los derechos de propiedad intelectual de la información	G	2	L1-L2	L2	L2
[D.3.4] Se dispone de normativa de retención de datos	G	3	L2	L3	L3
[D.I] Protección de la integridad	G	5			L3
[D.5] Protección de la confidencialidad	G	5	_-L3	_-L3	L2-L3
[D.C] Cifrado de la información	G	5	L0-L3	L2-L3	L2-L3

[D.C.1] Se dispone de normativa relativa al uso de cifra	G	2	L0-L1	L2	L2
[D.C.2] Se dispone de procedimientos relativos al cifrado de información	G	2	L1	L2	L2
[D.C.3] Se han designado responsables	G	2	L0	L2	L2
[D.C.4] Mecanismo de cifrado	T	5	L1-L3	L2-L3	L3
[D.5.2] Limpieza de documentos publicados	G	4	L0	L2	L3
[D.5.3] Marcado de la información	G	5			L3
[D.5.3.1] Marcado visible a efectos disuasorios	G	5			L3
[D.5.3.2] Marcado a efectos de detección y persecución	G	5			L3
[D.backup] Copias de seguridad (backups)	G	5	_-L3	_-L3	L3
[D.backup.1] Protección de la información	G	5	_-L1	_-L3	L3
[D.backup.1.1] Las copias de seguridad se protegen de acuerdo a la información que contienen	G	5	L1	L3	L3
[D.backup.1.2] Se cifran las copias de seguridad	G	4			L3
[D.backup.1.3] El acceso a las copias de seguridad requiere autorización previa	G	3	L1	L2	L3
[D.backup.2] Protección de la disponibilidad de la información	G	5	L0-L3	L2-L3	L3
[D.backup.2.1] Se dispone de normativa relativa a copias de seguridad (backup)	G	5	L2	L3	L3
[D.backup.2.2] Se dispone de procedimientos para las tareas de realización de copias de seguridad (backup), su protección y su conservación	G	5	L2	L3	L3
[D.backup.2.3] Gestión de las copias de seguridad de los datos (backup)	G	5	L0-L3	L2-L3	L3
[D.backup.2.3.1] Se hacen copias de la información en consonancia con sus requisitos de disponibilidad	G	3	L3	L3	L3
[D.backup.2.3.2] Se hacen copias de las claves para descifrar	G	5	L0	L2	L3
[D.backup.2.3.3] Se hacen copias de la información de verificación de firmas	G	5	L0	L2	L3
[D.backup.2.3.4] Las copias de seguridad, y los procedimientos, se almacenan en lugares diferentes de tal forma que los datos originales y las copias no se vean afectados simultáneamente por un incidente	G	4 (o)	L3	L3	L3
[D.backup.2.3.5] Periódicamente, se verifican las copias de seguridad	G	5	L0	L2	L3
[D.backup.2.3.6] Periódicamente, se prueban los procedimientos de restauración	G	3	L2	L3	L3
[D.backup.2.4] {xor} Mecanismo de backup	T	5	L2-L3	L3	L3
[D.DS] Uso de firmas electrónicas	T	6	L0-L3	L2-L3	L2-L4
[D.DS.1] Se dispone de normativa sobre firma electrónica	T	2	L0-L2	L2	L2
[D.DS.2] Se dispone de procedimientos para las trareas relacionadas con el empleo de firmas electrónicas	T	2	L1	L2	L2
[D.DS.3] Se han designado responsables	T	2	L0	L2	L2
[D.DS.4] Se garantiza la eficacia probatoria de la firma	T	3	L1	L2	L3

[D.DS.5] {xor} Certificados electrónicos	T	5	L3	L3	L3
[D.DS.6] {xor} Implantación de los algoritmos	T	5	L2	L2	L3
[D.DS.8] Se revisan regularmente las vulnerabilidades de los algoritmos	T	3	L1	L2	L3
[D.DS.9] Se emplean algoritmos certificados / acreditados	T	4	L2	L2	L3
[D.DS.a] Se emplean productos o servicios certificados o acreditados	T	5	L2	L2	L3
[D.TS] Uso de servicios de fechado electrónico (time stamping)	G	5	L0-L3	L1-L3	L2-L3
[D.TS.1] Se dispone de normativa de fechado electrónico	G	3	L0-L2	L1-L2	L2-L3
[D.TS.2] Se dispone de procedimientos para las tareas de fechado	G	2	L0	L1	L2
[D.TS.3] Se han designado responsables	G	2	L0	L2	L2
[D.TS.4] Se garantiza la eficacia probatoria del sello de tiempo	G	3	L3	L3	L3
[D.TS.6] {xor} Mecanismo de fechado electrónico	T	5	L2	L2	L3
[D.TS.7] Se revisan regularmente las vulnerabilidades de los algoritmos	G	3	L0	L1	L3
[D.TS.8] Se emplean productos o servicios certificados o acreditados	T	3	L3	L3	L3

Comentarios

[D] Protección de la Información

[D.TS] Uso de servicios de fechado electrónico (time stamping)

[D.TS.4] Se garantiza la eficacia probatoria del sello de tiempo

[actual] situación actual:

L'eficàcie del segell de temps la dóna CATCERT així que per això posem un L3

[K] Gestión de claves criptográficas

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[K.comms] Gestión de claves de comunicaciones	G	8	L0-L3	L1-L3	L2-L5
[K.comms.1] Se dispone de normativa de gestión de claves	G	3	L0	L2	L3
[K.comms.2] Se dispone de procedimientos de gestión de claves	G	3	L0	L1	L3
[K.comms.3] Se identifica la persona responsable de cada clave	G	3	L1	L2	L3
[K.comms.4] Operación	G	6	L2	L3	L3-L4
[K.comms.6] {xor} Generación de claves	T	5	L3	L3	L3
[K.comms.9] Las claves se destruyen de forma segura	T	5	L0	L2	L3
[K.comms.a] Se retienen copias de las claves	G	6	L0	L1	L2-L4

[S] Protección de los Servicios

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**

[S.1] Uso de los servicios	G	5	_-L3	_-L3	L2-L3
[S.1.1] Se dispone de normativa relativa al uso de los servicios	G	3	L3	L3	L3
[S.1.2] Se dispone de un registro de servicios a usuarios	G	3			L3
[S.1.3] Uso del correo electrónico (e-mail)	G	4	L0-L3	L2-L3	L2-L3
[S.1.3.1] Se dispone de normativa de uso	G	3	L1-L2	L2-L3	L2-L3
[S.1.3.2] Se detectan casos de uso inaceptable	T	4	L1	L2	L3
[S.1.3.3] Se verifica regularmente que se cumple la política	G	4	L0	L2	L3
[S.1.3.4] Se forma a los usuarios en el uso de los servicios	G	3	L0-L1	L2	L3
[S.1.3.5] Se dispone de un procedimiento de actuación en caso de incumplimiento	G	3	L1	L2	L3
[S.1.3.6] Se aplican medidas disciplinarias en caso de incumplimiento	G	3	L1	L2	L3
[S.1.3.7] Protección de la información	G	4	L0	L2	L3
[S.1.3.7.1] Se protege la información en el cuerpo del mensaje	T	4	L0	L2	L3
[S.1.3.7.2] Se protege la información adjunta al mensaje	T	4	L0	L2	L3
[S.1.3.8] Medidas frente a la recepción de spam	G	4	L3	L3	L3
[S.1.3.9] Medidas frente a código dañino en los clientes de correo	G	4	L3	L3	L3
[S.1.3.a] Software de prestación del servicio	T	4	L1-L2	L2-L3	L3
[COM.Internet] Navegación web	G	5	_-L1	_-L2	L2-L3
[COM.Internet.1] Se dispone de normativa de uso	G	3	_-L1	_-L2	L2-L3
[COM.Internet.2] Herramienta de monitorización del tráfico	G	2			L2
[COM.Internet.3] Herramienta de control de contenidos con filtros actualizados	T	5			L3
[COM.Internet.4] Se registra la navegación web	G	2			L2
[COM.Internet.5] Se han instalado herramientas anti spyware	G	4			L3
[COM.Internet.6] Se deshabilitan las 'cookies' en los navegadores	G	3			L3
[COM.Internet.7] Se controla la ejecución de código móvil (ej. 'applets')	T	4			L3
[COM.Internet.8] Software de prestación del servicio	T	3			L2-L3
[COM.Internet.8.1] Se designa el responsable para la administración del software	T	2			L2
[COM.Internet.8.2] Se configuran de forma segura los protocolos autorizados	T	3			L3
[COM.Internet.8.3] Se comprueba la publicación de actualizaciones por parte del proveedor	T	3			L3
[COM.Internet.8.4] El SW se actualiza regularmente (parches, versiones, etc.)	T	3			L3
[S.TW] Teletrabajo	G	4	L0-L2	L1-L2	L2-L3
[S.TW.1] Se ha designado al responsable de la administración del servicio	G	2	L0	L1	L2

[S.TW.2] Se dispone de normativa de uso	G	3	L0	L1	L2-L3
[S.TW.3] Se forma a los usuarios en el uso de los servicios	G	2	L0	L1	L2
[S.TW.4] Se detectan casos de uso inaceptable	T	3	L0	L1	L3
[S.TW.5] Se verifica regularmente que se cumple la política	G	4	L0	L1	L3
[S.TW.6] Se dispone de procedimientos para gestión del teletrabajo	G	3	L0	L1	L2-L3
[S.TW.7] Se aplican medidas disciplinarias en caso de incumplimiento	G	2	L0	L1	L2
[S.TW.8] Se requiere autorización previa	G	2	L2	L2	L2
[S.TW.9] Estudio de las características específicas del emplazamiento	G	4	L0	L1	L2-L3
[S.TW.9.1] Se analiza la seguridad física	G	3	L0	L1	L3
[S.TW.9.2] Se analiza el entorno	F	3	L0	L1	L3
[S.TW.9.3] Se previene el uso del puesto por otras personas (acceso no autorizado)	G	3	L0	L1	L3
[S.TW.9.4] Seguridad del puesto de usuario	T	4	L0	L1	L2-L3
[S.TW.9.5] Instalación de software por parte de los usuarios	T	3	L0	L1	L3
[S.TW.9.6] Seguridad de las comunicaciones	G	3	L0	L1	L3
[S.TW.9.7] Conexión a redes particulares por parte de los usuarios	T	3	L0	L1	L3
[S.2] Prestación de los servicios	G	6	_-L3	_-L3	L2-L4
[S.2.1] Se dispone de un inventario de servicios	G	2	L0-L1	L2	L2
[S.cont] Aseguramiento de la disponibilidad	G	4	_-L2	_-L3	L2-L3
[S.cont.1] Protección frente a ataques de denegación de servicio (DoS)	G	3			L2-L3
[S.cont.2] Gestión de recursos	G	4	L2	L3	L3
[S.cont.2.1] Se han dimensionado los dispositivos accesibles (cortafuegos, servidores, ...) para soportar la máxima carga prevista	G	4	L2	L3	L3
[S.cont.2.2] Se ha dimensionado adecuadamente la capacidad de almacenamiento de los dispositivos de registro (logs) de actividad	G	3	L2	L3	L3
[S.cont.2.3] Los recursos se priorizan en base a la prioridad del servicio afectado	T	3	L2	L3	L3
[S.start] Aceptación y puesta en operación	G	4	L0-L2	L1-L3	L2-L3
[S.SC] Se aplican perfiles de seguridad	T	6	_-L2	_-L3	L3-L4
[S.op] Explotación	G	4	_-L0	_-L2	L3
[S.op.1] Se realizan análisis periódicos de vulnerabilidades	G	4			L3
[S.op.2] Se detectan casos de intrusión en el servicio	G	4			L3
[S.op.3] Prevención del repudio	T	4	L0	L2	L3
[S.op.4] El personal recibe formación específica en configuración de servicios	G	3			L3
[S.CM] Gestión de cambios (mejoras y sustituciones)	G	3	L0-L3	L1-L3	L2-L3
[S.CM.1] Se dispone de normativa de control de cambios	G	2	L0	L2	L2

[S.CM.2] Se designan responsables	G	2	L0-L1	L2	L2
[S.CM.3] Se dispone de procedimientos para ejecutar cambios	G	2	L0-L2	L2	L2
[S.CM.4] Se hace un seguimiento permanente (servicios externos)	G	3	L0	L2	L3
[S.CM.5] Evaluación del impacto potencial del cambio	G	2	L1-L2	L2	L2
[S.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	G	3	L3	L3	L3
[S.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	G	3	L3	L3	L3
[S.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	G	3	L1	L2	L3
[S.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	G	2	L2	L2	L2
[S.CM.a] Se realiza por personal debidamente autorizado	G	3	L3	L3	L3
[S.CM.b] Se realizan pruebas de regresión	T	2	L0	L1	L2
[S.CM.c] Se registran las actualizaciones de servicios	G	2	L0	L2	L2
[S.CM.d] Documentación	G	2	L0	L1	L2
[S.CM.e] Se actualizan todos los procedimientos de producción afectados	G	2	L0	L1	L2
[S.CM.f] Se actualizan todos los procedimientos de recuperación afectados	G	1	L0	L1	L2
[S.end] Desmantelamiento	G	4			L2-L3
[S.2.a] Seguridad del comercio electrónico	G	4	L2	L2-L3	L2-L3
[S.2.a.1] Se tienen en cuenta los requisitos	T	2	L2	L2	L2
[S.2.a.2] Redacción y aprobación de un documento que consigne los términos acordados entre las partes	T	2	L2	L2	L2
[S.2.a.3] Controles sobre el desarrollo del proceso (fijación de precios, contratación, etc.)	T	3	L2	L3	L3
[S.2.a.4] Implantación de mecanismos de autenticación de las partes	T	4	L2	L3	L3
[S.2.a.5] Establecimiento de mecanismos de autorización del proceso	T	3	L2	L3	L3
[S.2.a.6] Se dispone de un registro de actividades	T	3	L2	L2	L3
[S.3] Servicios subcontratados	G	6	L0-L3	L1-L3	L2-L4
[S.3.1] Aspectos generales	G	2	L2-L3	L2-L3	L2
[S.3.1.1] Se dispone de un registro de servicios subcontratados	G	2	L2	L2	L2
[S.3.1.2] Se requiere aprobación previa para el uso de servicios externos	G	2	L3	L3	L2
[S.3.1.3] Se identifican las aplicaciones sensibles o críticas que debe retener la Organización	G	2	L2	L2	L2
[S.3.1.4] Se identifican los riesgos derivados de depender de un proveedor externo	G	2	L2	L2	L2
[S.3.2] Contratos de prestación de servicios	G	3	L0-L3	L1-L3	L2-L3
[S.3.2.1] Se define la política aplicable sobre seguridad de la información	G	2	L1	L2	L2
[S.3.2.2] Constan las obligaciones de todas las partes	G	2	L1	L2	L2

[S.3.2.3] Se incluyen los requisitos de seguridad	G	3	L1	L2	L2-L3
[S.3.2.4] Se define, y se incorpora al contrato el procedimiento para medir el cumplimiento de las medidas de seguridad	G	2	L0	L1	L2
[S.3.2.5] IPR: Se contemplan los temas relativos a propiedad intelectual	G	2	L0	L1	L2
[S.3.2.6] Se contempla la protección de la información de carácter personal	G	2	L3	L3	L2
[S.3.2.7] Se establecen los términos para la implicación de terceros (subcontratistas)	G	2	L2	L2	L2
[S.3.2.8] Se describen los servicios disponibles	G	2	L0	L1	L2
[S.3.2.9] Se definen las responsabilidades sobre instalación y mantenimiento de HW y SW	G	2	L0	L1	L2
[S.3.2.a] Se definen las responsabilidades en la supervisión del cumplimiento del contrato	G	2	L0	L1	L2
[S.3.3] Operación	G	6	L0-L2	L1-L3	L2-L4
[S.3.4] Gestión de cambios	G	2	L1-L2	L2	L2
[S.3.5] Autenticación del servidor	T	4	L0-L3	L2-L3	L2-L3
[S.3.5.1] Se autentica el servidor antes de transferir información alguna	T	4	L2	L3	L3
[S.3.5.2] {xor} Mecanismo de autenticación	T	3	L3	L3	L3
[S.3.5.2.1] Secreto compartido	T	3	L3	L3	L3
[S.3.5.2.1.1] Se protege el secreto en el cliente	T	3	L3		L3
[S.3.5.2.1.2] Robusto frente a ataques de fuerza bruta	T	3	L3		L3
[S.3.5.2.1.3] Se protege el canal de autenticación	T	3	L3		L3
[S.3.5.2.2] Criptografía: firma digital	T	3			L3
[S.3.5.2.2.1] Se protegen los datos de validación en el cliente	T	3			L3
[S.3.5.2.2.2] Se emplean algoritmos certificados o acreditados	T	3			L3
[S.3.5.3] Protección de datos y software de autenticación	T	3	L2-L3	L2-L3	L2-L3
[S.3.5.3.1] {xor} Implementación del mecanismo	T	3	L3	L3	L3
[S.3.5.3.1.1] por programa (SW)	T	3	L3	L3	L3
[S.3.5.3.2] Se protege el uso por medio de contraseña	T	1	L2	L2	L2
[S.3.5.3.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	3	L2	L3	L3
[S.3.5.3.4] Se usa un producto certificado o acreditado	T	3	L2	L3	L3
[S.3.5.4] Se toman medidas para impedir el secuestro de sesiones establecidas	T	3	L0	L2	L3
[S.3.6] Continuidad de operaciones	G	2	L1	L2	L2
[S.3.7] Desmantelamiento	G	4	L1	L2	L2-L3
[S.3.7.1] Se requiere autorización previa	G	2	L1	L2	L2
[S.3.7.2] Se estudia el impacto en el negocio	G	1	L1	L2	L2
[S.3.7.3] Se planifica de forma que minimice la interrupción del servicio	G	2	L1	L2	L2
[S.3.7.4] Destrucción de la información en el proveedor	G	4	L1	L2	L3
[S.3.7.5] Desactivación del servicio por personal	G	3	L1	L2	L3

autorizado					
[S.3.7.6] Se actualizan todos los procedimientos de producción afectados	G	2	L1	L2	L2
[S.3.7.7] Se actualizan todos los procedimientos de recuperación afectados	G	1	L1	L2	L2

[SW] Protección de las Aplicaciones Informáticas (SW)

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[SW.1] Se dispone de un inventario de aplicaciones (SW)	G	2	L0-L2	L1-L2	L2
[SW.2] Se dispone de normativa relativa a las aplicaciones (SW)	G	2	L0	L2	L2
[SW.3] Se dispone de procedimientos de uso de las aplicaciones	G	2	L1	L2	L2
[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)	G	3	L1-L2	L2	L2-L3
[SW.backup] Copias de seguridad (backup) (SW)	G	4	L1-L2	L2-L3	L2-L3
[SW.start] Puesta en producción	G	4	L0-L2	L1-L3	L2-L3
[SW.SC] Se aplican perfiles de seguridad	T	7	L0-L3	L2-L3	L3-L4
[SW.op] Explotación / Producción	G	5	L0-L3	L1-L3	L2-L3
[SW.op.1] Se dispone de normativa relativa al software en producción	G	2	L0	L2	L2
[SW.op.2] Los sistemas de producción no contienen herramientas de desarrollo	G	4	L2	L3	L3
[SW.op.3] {xor} Se controla la integridad del código ejecutable	G	4	L0	L2	L3
[SW.op.4] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	T	3 (o)	L1	L2	L3
[SW.op.5] Aislamiento de sistemas que manejen asuntos delicados	G	3	L1-L2	L1-L2	L2-L3
[SW.op.6] Seguridad de las aplicaciones	G	4	L0-L1	L1-L2	L2-L3
[SW.op.6.1] Validación de los datos de entrada	G	4	L0-L1	L2	L2-L3
[SW.op.6.2] Se verifica la consistencia interna de los datos	G	4	L0-L1	L1-L2	L2-L3
[SW.op.6.3] Validación de los datos de salida	G	3	L0	L1	L2-L3
[SW.op.7] Seguridad de los ficheros de datos de la aplicación	T	4	L2	L2	L2-L3
[SW.op.8] Se protegen los ficheros de configuración	T	5	L1	L2	L2-L3
[SW.op.9] Se protegen los ficheros del sistema	T	4	L1-L2	L2	L2-L3
[SW.op.a] Se controla la ejecución de código móvil (ej. 'applets')	T	3	L1-L2	L2-L3	L2-L3
[SW.op.b] Ejecución de programas colaborativos (ej. teleconferencia)	T	3	L3	L3	L3
[SW.op.c] Seguridad de los mecanismos de comunicación entre procesos	T	5	L1	L2	L3
[SW.op.d] Regularmente se realiza un análisis de vulnerabilidades, y se actúa en consecuencia	G	3	L2	L3	L3
[SW.op.e] Formación del personal en configuración de	G	2	L2	L2	L2

aplicaciones					
[SW.CM] Cambios (actualizaciones y mantenimiento)	G	4	L0-L3	L1-L3	L2-L3
[SW.CM.1] Se dispone de una política	G	2	L0-L2	L1-L2	L2
[SW.CM.2] Se dispone de procedimientos para ejecutar cambios	G	2	L0-L2	L1-L2	L2
[SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches	G	3	L2	L3	L3
[SW.CM.4] Evaluación del impacto y riesgo residual tras el cambio	G	2	L0	L1	L2
[SW.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	G	4	L3	L3	L3
[SW.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	G	3	L3	L3	L3
[SW.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	G	3	L3	L3	L3
[SW.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	G	3	L0	L1	L3
[SW.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	G	2	L2	L2	L2
[SW.CM.a] Control de versiones de toda actualización del software	G	3	L1	L2	L3
[SW.CM.b] Realización por personal debidamente autorizado	G	3	L3	L3	L3
[SW.CM.c] Se retienen copias de las versiones anteriores de software como medida de precaución para contingencias	G	2	L1	L2	L2
[SW.CM.d] Se retienen copias de las versiones anteriores de configuración	T	3	L0	L2	L3
[SW.CM.e] Se prueba previamente en un equipo que no esté en producción	T	3	L2	L3	L3
[SW.CM.f] Pruebas de regresión	T	3	L0	L1	L3
[SW.CM.g] Se registra toda actualización de SW	G	2	L0	L2	L2
[SW.CM.h] Documentación	G	2	L0	L2	L2
[SW.CM.i] Se actualizan todos los procedimientos de producción afectados	G	3	L0	L2	L3
[SW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	G	1	L0	L2	L2
[SW.end] Desmantelamiento	G	2			L2

[HW] Protección de los Equipos Informáticos (HW)

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[HW.1] Se dispone de un inventario de equipos (HW)	G	2	L1-L2	L2	L2
[HW.2] Se dispone de normativa sobre el uso correcto de los equipos	G	2	L3	L3	L2
[HW.3] Se dispone de procedimientos de uso del equipamiento	G	2	L1	L2	L2
[HW.start] Puesta en producción	G	4	L0-L2	L2-L3	L2-L3
[HW.SC] Se aplican perfiles de seguridad	T	7			L3-L4

[HW.cont] Aseguramiento de la disponibilidad	G	5	L1-L3	L2-L3	L2-L3
[HW.cont.1] Se dimensiona holgadamente y se planifica la adquisición de repuestos	G	5	L2	L3	L3
[HW.cont.2] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	G	3	L2	L3	L3
[HW.cont.3] El mantenimiento lo realiza personal debidamente autorizado	G	3	L3	L3	L3
[HW.cont.4] Se ejecutan regularmente las rutinas de diagnóstico	G	2	L1	L2	L2
[HW.cont.5] Se monitorizan fallos e incidentes	G	2	L1	L2	L2
[HW.cont.6] Se registran los fallos, reales o sospechados y de mantenimiento preventivo y correctivo	G	2	L2	L2	L2
[HW.cont.7] Se hacen copias de seguridad de la configuración	G	2	L1	L2	L2
[HW.cont.8] Se hacen copias de seguridad de las claves de descifrado	G	3	L1	L2	L3
[HW.cont.9] {xor} Opciones sustitutorias	G	3	L3	L3	L3
[HW.cont.9.1] Equipo alternativo	G	3	L3	L3	L3
[HW.cont.9.2] Equipo alternativo preconfigurado con replicación de discos síncrona o asíncrona	G	3			L3
[HW.cont.9.3] Sistema redundante propio en centro alternativo	G	3	L3	L3	L3
[HW.cont.9.4] Contrato de prestación de servicio con el proveedor del sistema, de acuerdo a los requisitos del negocio	G	3			L3
[HW.cont.a] {xor} Alta disponibilidad	G	2	L3	L3	L2
[HW.cont.b] Las medios alternativos están sujetos a las mismas garantías de protección que los habituales	G	2	L2	L2	L2
[HW.cont.c] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento	G	2	L2	L2	L2
[HW.7] Contenedores criptográficos (HW, HW virtual)	G	6	_-L2	_-L2	L3-L4
[HW.9] Instalación	G	3	L2-L3	L3	L3
[HW.op] Operación	G	4	_-L3	_-L3	L2-L3
[HW.op.1] Proceso de autorización de recursos para el tratamiento de la información	G	2	L2	L2	L2
[HW.op.2] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	T	3 (o)			L3
[HW.op.3] Protección física de los equipos	F	4	L0-L3	L2-L3	L3
[HW.op.4] Seguridad del equipamiento de oficina	G	3			L2-L3
[HW.op.5] Seguridad de los equipos fuera de las instalaciones	F	4	L0	L1-L2	L2-L3
[HW.op.6] Protección de los dispositivos de red	G	3	_-L3	_-L3	L2-L3
[HW.op.8] Formación del personal en configuración de equipos	G	2			L2
[HW.CM] Cambios (actualizaciones y mantenimiento)	G	4	L0-L3	L1-L3	L2-L3
[HW.CM.1] Se dispone de una política	G	2	L0-L1	L2	L2
[HW.CM.2] Se dispone de procedimientos para ejecutar cambios	G	2	L0-L2	L2	L2

[HW.CM.3] Se siguen las recomendaciones del fabricante o proveedor	G	3	L3	L3	L3
[HW.CM.4] Se hace un seguimiento permanente de actualizaciones	G	3	L2	L3	L3
[HW.CM.5] Evaluación del impacto potencial del cambio	G	2	L1-L2	L2	L2
[HW.CM.6] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	G	4	L2	L3	L3
[HW.CM.7] Se mantiene en todo momento la regla de 'funcionalidad mínima'	G	3	L3	L3	L3
[HW.CM.8] Se mantiene en todo momento la regla de 'seguridad por defecto'	G	3	L2	L3	L3
[HW.CM.9] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	G	3	L1	L2	L3
[HW.CM.a] Se planifica el cambio de forma que minimice la interrupción del servicio	G	2	L2	L2	L2
[HW.CM.b] Realización por personal debidamente autorizado	G	3	L3	L3	L3
[HW.CM.c] Se retienen copias de las versiones anteriores de configuración	T	3	L2	L3	L3
[HW.CM.d] Se prueba previamente en un entorno que no esté en producción	T	3	L2	L3	L3
[HW.CM.e] Pruebas de regresión	T	3	L0	L1	L3
[HW.CM.f] Todos los cambios quedan registrados	G	2	L0	L2	L2
[HW.CM.g] Documentación	G	2	L0	L1	L2
[HW.CM.h] Control de versiones de todo cambio de hw	G	2	L0	L1	L2
[HW.CM.i] Se actualizan todos los procedimientos de producción afectados	G	3	L0	L2	L3
[HW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	G	1	L0	L2	L2
[HW.end] Desmantelamiento	G	2	L0	L2	L2
[HW.PCD] Informática móvil	G	3	L0-L2	L1-L2	L2-L3
[HW.PCD.1] Se mantiene un inventario de equipos móviles con identificación del responsable de cada uno	G	2	L0	L2	L2
[HW.PCD.2] Se requiere autorización previa antes de poder usarlos	G	2	L0	L1	L2
[HW.PCD.3] Cada equipo se marca con el nivel máximo de información que puede almacenar o procesar	G	2	L0	L1	L2
[HW.PCD.4] Se han identificado los riesgos correspondientes	G	2	L0	L1	L2
[HW.PCD.5] Se han determinado las medidas y precauciones a tomar	G	3	L0-L1	L1-L2	L2-L3
[HW.PCD.6] Se sigue un plan de concienciación sobre los riesgos y las medidas pertinentes	G	2	L1	L2	L2
[HW.PCD.7] Se sigue un plan de formación sobre las medidas pertinentes	G	2	L1	L2	L2
[HW.PCD.8] Controles aplicables	G	3	L0-L2	L1-L2	L2-L3
[HW.PCD.8.1] Se han determinado las medidas para la protección física del dispositivo	G	3	L0	L1	L3

[HW.PCD.8.2] Se instalan detectores de violación	G	3	L0	L1	L3
[HW.PCD.8.3] Se han establecido los requisitos sobre control de acceso	G	3	L0	L1	L3
[HW.PCD.8.4] Se utiliza un sistema de defensa perimetral (cortafuegos)	G	3	L0	L1	L3
[HW.PCD.8.5] Se han establecido los requisitos de cifrado	G	3	L0	L1	L3
[HW.PCD.8.6] Se han establecido los requisitos sobre copias de seguridad (backups)	G	2	L0	L1	L2
[HW.PCD.8.7] Se instala software antivirus y se mantiene actualizado	G	3	L2	L2	L3
[HW.PCD.9] Guías para los usuarios	G	2	L0	L2	L2
[HW.PCD.a] Gestión de incidentes en informática móvil	G	3	L2	L2	L2-L3
[HW.e] Maquinas virtuales	G	4			L2-L3
[HW.e.1] Para la creación de nuevas máquinas virtuales se requiere autorización previa	G	2			L2
[HW.e.2] Se controla el hypervisor	G	3			L3
[HW.e.2.1] Se controla el acceso al hyperviror	G	3			L3
[HW.e.2.2] Se controla el acceso a recursos compartidos	G	3			L3
[HW.e.3] Se controla el acceso a las imágenes de las máquinas virtuales	G	3			L3
[HW.e.4] Se protegen las copias de seguridad de las imágenes de las máquinas virtuales	G	3			L3
[HW.e.5] No se instalan sobre el mismo equipo anfitrión servidores y clientes virtuales	G	3			L3
[HW.e.6] No se instalan sobre el mismo equipo anfitrión equipos de frontera y equipos internos (ej. cortafuegos, pasarelas, etc.)	G	4			L3
[HW.e.7] Retirada de servicio	G	3			L2-L3
[HW.e.7.1] Se registra la retirada del servicio	G	2			L2
[HW.e.7.2] {xor} Se aplican al soporte de la imagen virtual los mecanismos previstos para soportes de información	G	3			L3
[HW.print] Reproducción de documentos	G	3			L2-L3
[HW.print.1] Control de los dispositivos de reproducción (fotocopiadoras, fax, etc.)	G	3			L3
[HW.print.2] Asignación de cuentas de usuario	G	3			L3
[HW.print.3] Destrucción ó borrado seguro de las partes de los dispositivos de reproducción que puedan contener información previamente a su sustitución	G	3			L3
[HW.print.4] Se requiere autorización previa para realizar copias, y numeración de las mismas	G	2			L2
[HW.print.5] Se registra y se revisa la actividad de los dispositivos de reproducción (número de copias, usuarios que las han realizado, etc.)	G	3			L3
[HW.h] Voz, facsímil y video	G	3			L2-L3
[HW.h.1] Está prohibido establecer de conversaciones confidenciales en lugares públicos o sin adecuadas	G	3			L3

medidas de protección					
[HW.h.2] Está prohibido dejar mensajes confidenciales en contestadores automáticos	G	3			L3
[HW.h.3] Los usuarios están concienciados y reciben formación sobre el uso seguro de los sistemas y recursos disponibles	G	2			L2
[HW.h.4] Se controla el acceso a la memoria interna del equipo de fax	G	3			L3
[HW.h.5] Se prohíbe la programación no autorizada del equipo de fax	G	3			L3
[HW.h.6] Se previene el envío de documentos a números equivocados	G	3			L3

[COM] Protección de las Comunicaciones

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[COM.1] Se dispone de un inventario de servicios de comunicación	G	2	L1-L2	L2	L2
[COM.2] Se dispone de normativa sobre el uso correcto de las comunicaciones	G	3	L1	L2	L3
[COM.3] Se dispone de procedimientos de uso de las comunicaciones	G	3	L1	L2	L3
[COM.start] Entrada en servicio	G	4	L0-L2	L2-L3	L2-L3
[COM.SC] Se aplican perfiles de seguridad	T	8	L2-L3	L3	L3-L5
[COM.cont] Aseguramiento de la disponibilidad	G	5	L0-L3	L2-L3	L2-L3
[COM.cont.1] Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)	G	5	L3	L3	L3
[COM.cont.2] Se dimensiona holgadamente y se planifica la adquisición de repuestos	G	3	L2	L3	L3
[COM.cont.3] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	G	4	L3	L3	L3
[COM.cont.4] Se monitorizan enlaces y dispositivos de red	G	4	L3	L3	L3
[COM.cont.5] Se registran los fallos detectados, sean reales o sospechados	G	1	L1	L2	L2
[COM.cont.6] Se registran las actuaciones de mantenimiento preventivo y correctivo	G	1	L0	L2	L2
[COM.cont.7] Se realizan copias de seguridad de la configuración (backup)	G	4	L1	L2	L3
[COM.cont.8] Se hacen copias de seguridad de las claves de autenticación	G	4	L2	L3	L3
[COM.cont.9] Se hacen copias de seguridad de las claves de descifrado	G	4	L2	L3	L3
[COM.cont.a] {xor} Redundancia	T	4	L3	L3	L3
[COM.cont.b] Las medios alternativos están sujetos a las mismas garantías de protección que los habituales	G	2	L2	L2	L2
[COM.cont.c] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento	G	2	L2	L2	L2
[COM.aut] Autenticación del canal	T	5	L0-L3	L2-L3	L2-L3

[COM.aut.1] Se requiere autorización previa	T	2	L2	L2	L2
[COM.aut.2] Se verifica la identidad del usuario antes de entregarle el mecanismo de autenticación	T	3	L2	L2	L3
[COM.aut.3] Se autentica el origen de la conexión	T	3	L2	L2	L3
[COM.aut.4] {xor} Mecanismo de autenticación	T	5	L3	L3	L3
[COM.aut.4.2] Certificados software (criptografía de clave pública)	T	5	L3	L3	L3
[COM.aut.4.3] 2 factores: token + contraseña	T	5	L1-L3	L1-L3	L2-L3
[COM.aut.4.3.1] Token físico - algo que se tiene	T	4	L1-L3	L1-L3	L2-L3
[COM.aut.4.3.1.1] El usuario asume la responsabilidad de la custodia del token	T	2	L3	L3	L2
[COM.aut.4.3.1.2] Difícil de clonar	T	4	L3	L3	L3
[COM.aut.4.3.1.3] Cuando no se emplea, el token se guarda en lugar separado seguro	T	4	L1	L1	L3
[COM.aut.4.3.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5	L3	L3	L3
[COM.aut.4.4] 2 factores: token + certificados	T	5	L3	L3	L2-L3
[COM.aut.4.4.1] Token físico - algo que se tiene	T	4	L3	L3	L2-L3
[COM.aut.4.4.1.1] El usuario asume la responsabilidad de la custodia del token	T	2	L3	L3	L2
[COM.aut.4.4.1.2] Difícil de clonar	T	4	L3	L3	L3
[COM.aut.4.4.1.3] Cuando no se emplea, el token se guarda en lugar separado seguro	T	4	L3	L3	L3
[COM.aut.4.4.2] Se protege el uso por medio de contraseña	T	3	L3	L3	L3
[COM.aut.4.4.3] El certificado se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5	L3	L3	L3
[COM.aut.4.4.4] Gestión de los certificados	T	4	L3	L3	L3
[COM.aut.4.4.4.1] Los certificados se revocan al ser comprometidos o existir sospecha de ello	T	4	L3	L3	L3
[COM.aut.4.4.4.2] Los certificados tienen una validez limitada y se renuevan periódicamente	T	4	L3	L3	L3
[COM.aut.4.4.5] Se usa un producto certificado o acreditado	T	3	L3	L3	L3
[COM.aut.4.4.6] Se emplean algoritmos certificados / acreditados	T	3	L3	L3	L3
[COM.aut.4.4.7] Se emplean parámetros certificados / acreditados	T	3	L3	L3	L3
[COM.aut.4.5] 2 factores: contraseña de un solo uso (OTP) con token	T	5	L3	L3	L3
[COM.aut.4.5.1] El usuario asume la responsabilidad de la custodia del token	T	3	L3	L3	L3
[COM.aut.4.5.2] Difícil de clonar	T	4	L3	L3	L3
[COM.aut.4.5.3] Cuando no se emplea, el token se guarda en lugar separado seguro	T	4	L3	L3	L3
[COM.aut.4.5.4] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5	L3	L3	L3
[COM.aut.4.5.5] Se usa un producto certificado o acreditado	T	3	L3	L3	L3

[COM.aut.4.6] 2 factores: contraseña de un solo uso (OTP) por canal separado	T	5	L3	L3	L3
[COM.aut.4.6.1] Canal de comunicación separado (e.g. SMS)	T	4	L3	L3	L3
[COM.aut.4.6.1.1] Se protege frente a ataques de interceptación pasiva	T	4	L3	L3	L3
[COM.aut.4.6.1.2] Se protege frente a ataques de interceptación activa	T	4	L3	L3	L3
[COM.aut.4.6.1.3] Se protege el dispositivo de recepción	T	4	L3	L3	L3
[COM.aut.4.6.2] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5	L3	L3	L3
[COM.aut.5] Canal de autenticación	T	4	L0	L2	L3
[COM.aut.6] Se toman medidas para impedir el secuestro de sesiones establecidas	T	3	L0	L2	L3
[COM.I] {xor} Protección de la integridad de los datos intercambiados	T	5	L2	L3	L3
[COM.9] Se toman medidas frente a la inyección de información espuria	T	5			L3
[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados	G	5	L1-L2	L2-L3	L3
[COM.C.1] Se dispone de normativa relativa al uso de controles criptográficos	G	4	L1	L2	L3
[COM.C.2] Se han designado responsables	G	4	L1	L2	L3
[COM.C.3] {xor} Implantación de los algoritmos	T	4	L1	L2	L3
[COM.C.4] {xor} Mecanismo de cifrado (secreto compartido o cifra simétrica)	T	4	L2	L3	L3
[COM.C.5] Se revisan regularmente las vulnerabilidades de los algoritmos	G	5	L1	L2	L3
[COM.C.6] Se emplean algoritmos certificados / acreditados	T	5	L1	L2	L3
[COM.C.7] Se emplean productos o servicios certificados o acreditados	T	5	L2	L3	L3
[COM.op] Operación	T	4	L1-L3	L2-L3	L2-L3
[COM.op.1] Control de acceso a la red	T	4	L1-L3	L2-L3	L2-L3
[COM.op.1.1] Se dispone de normativa de uso de los servicios de red	T	2	L1	L2	L2
[COM.op.1.2] Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios	T	2	L2	L2	L2
[COM.op.1.3] Acceso remoto	T	4	L1-L3	L2-L3	L2-L3
[COM.op.1.4] {xor} Protección de los puertos de diagnóstico remoto	T	4	L1	L2	L3
[COM.op.1.6] Control del encaminamiento	T	3	L3	L3	L3
[COM.op.2] Seguridad de los servicios de red	T	4	L2	L3	L3
[COM.op.2.1] Se monitorizan los servicios de red	T	3	L2	L3	L3
[COM.op.2.2] Revisiones periódicas de la seguridad	T	4	L2	L3	L3
[COM.op.3] Se prevé protección frente a análisis del tráfico	T	4	L3	L3	L3
[COM.op.4] Formación del personal en configuración de	T	3	L3	L3	L3

las comunicaciones					
[COM.CM] Cambios (actualizaciones y mantenimiento)	G	5	L0-L3	L1-L3	L2-L3
[COM.CM.1] Se dispone de una política	G	2	L0-L1	L2	L2
[COM.CM.2] Se dispone de procedimientos para ejecutar cambios	G	2	L0-L2	L2	L2
[COM.CM.3] Se hace un seguimiento permanente de actualizaciones	G	3	L2	L2	L3
[COM.CM.4] Evaluación del impacto y riesgo residual tras el cambio	G	2	L1-L2	L2	L2
[COM.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	G	5	L2	L3	L3
[COM.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	G	3	L3	L3	L3
[COM.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	G	3	L3	L3	L3
[COM.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	G	3	L1	L2	L3
[COM.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	G	1	L2	L2	L2
[COM.CM.a] Realización por personal debidamente autorizado	G	4	L3	L3	L3
[COM.CM.b] Se retienen copias de las versiones anteriores de configuración	T	3	L1	L2	L3
[COM.CM.c] Se prueba previamente en un entorno que no esté en producción	T	4	L1	L2	L3
[COM.CM.d] Pruebas de regresión	G	4	L0	L1	L3
[COM.CM.e] Todas las actuaciones quedan registradas	G	2	L0	L2	L2
[COM.CM.f] Documentación	G	2	L0	L1	L2
[COM.CM.g] Se actualizan todos los procedimientos de producción afectados	G	3	L0	L1	L3
[COM.CM.h] Se actualizan todos los procedimientos de recuperación afectados	G	1	L0	L1	L2
[COM.end] Desmantelamiento	G	3			L3
[COM.wifi] Seguridad Wireless (WiFi)	G	7	L0-L3	L2-L3	L3-L4
[COM.wifi.1] Se requiere autorización previa para desplegar puntos de acceso (AP)	G	3	L3	L3	L3
[COM.wifi.2] Al instalar un punto de acceso (AP) se tiene en cuenta el alcance de la señal para evitar una exposición gratuíta a ataques	G	3	L3	L3	L3
[COM.wifi.3] Se requiere autorización previa para la conexión de clientes	G	3	L3	L3	L3
[COM.wifi.5] Se desactivan los puertos y servicios no usados	G	4	L3	L3	L3
[COM.wifi.7] Se aplican restricciones al protocolo SNMP en redes wireless	G	4	L2	L3	L3
[COM.wifi.8] Se comprueban periódicamente los puntos de acceso (mediante broadcast o herramientas)	T	4	L1	L2	L3
[COM.wifi.9] Se desactiva el modo de conexión ad-hoc en los dispositivos de usuario	T	4	L0	L2	L3

[COM.wifi.a] Se autentican los dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)	T	5	L0	L2	L3
[COM.wifi.b] Se controlan las direcciones IP	G	4	L2	L3	L3
[COM.DS] Segregación de las redes en dominios	T	6	L3	L3	L3-L4

[IP] Puntos de interconexión: conexiones entre zonas de confianza

salvaguarda	A	R	[actual]	[objetivo]	[PILAR]
[IP.1] Administración	G	3	L1	L2	L2-L3
[IP.1.1] Las conexiones requieren autorización previa	G	2	L1	L2	L2
[IP.1.2] Se dispone de un inventario de conexiones autorizadas	G	2	L1	L2	L2
[IP.1.3] Se realiza una monitorización continua de las conexiones autorizadas	T	3	L1	L2	L3
[IP.1.4] Los usuarios y procesos autorizados a usar el enlace sólo disfrutan de los derechos mínimos imprescindibles	G	2	L1	L2	L2
[IP.1.5] Se revisan regularmente los usuarios y procesos autorizados	G	3	L1	L2	L3
[IP.2] Establecimiento de conexión	G	5	L2	L2	L3
[IP.2.1] Se identifican y autentican los usuarios antes de establecer el enlace	G	5	L2	L2	L3
[IP.2.2] Se identifican y autentican los procesos usuarios antes de establecer el enlace	G	5	L2	L2	L3
[IP.2.3] El servidor se identifica y autentica antes de establecer el enlace	G	5	L2	L2	L3
[IP.SPP] Tráfico: Intercambio de datos	T	4	L1-L3	L2-L3	L2-L3
[IP.SPP.1] Cualquier otro nodo de la red se considera no fiable, realizándose un control local de los datos intercambiados	T	2	L1	L2	L2
[IP.SPP.2] Se valida el formato de todos los datos en tránsito	T	3	L3	L3	L3
[IP.SPP.3] Tráfico autorizado	T	3	L2-L3	L3	L2-L3
[IP.SPP.3.1] El tráfico permitido requiere autorización previa	T	2	L3	L3	L2
[IP.SPP.3.2] El tráfico se identifica antes de autorizar su paso	T	3	L3	L3	L3
[IP.SPP.3.3] Se revisa periódicamente el tráfico autorizado	T	3	L2	L3	L3
[IP.SPP.4] Se controla el tráfico entrante y saliente	T	4	L1-L3	L2-L3	L2-L3
[IP.SPP.5] Intermediación - El punto de interconexión intermediará los siguientes procesos:	T	3	L3	L3	L3
[IP.SPP.5.1] Identificación y autenticación de los usuarios	T	3	L3	L3	L3
[IP.SPP.5.2] Identificación y autenticación de los nodos	T	3	L3	L3	L3
[IP.SPP.5.3] Autorización de acceso	T	3	L3	L3	L3
[IP.SPP.5.4] Listas blancas (white lists)	T	3	L3	L3	L3

[IP.SPP.5.5] Listas negras (black lists)	T	3	L3	L3	L3
[IP.SPP.5.6] Etiquetas de seguridad de los objetos intercambiados	T	3	L3	L3	L3
[IP.SPP.5.7] Información de control de red (nivel 3)	T	3	L3	L3	L3
[IP.SPP.5.8] Información de control de aplicación (nivel 7)	T	3	L3	L3	L3
[IP.SPP.6] Tráfico de gesión	T	3	L2	L2	L3
[IP.SPP.6.1] Se asegura la autenticidad del origen	T	3	L2	L2	L3
[IP.SPP.6.2] Se asegura la integridad de la información	T	3	L2	L2	L3
[IP.SPP.6.3] Se asegura la confidencialidad de la información	T	3	L2	L2	L3
[IP.SPP.7] Se ocultan las direcciones IP internas (servicio NAT o similar)	T	1	L2	L2	L2
[IP.SPP.8] Se ocultan los puertos internos (servicio PAT o similar)	T	1	L2	L2	L2
[IP.4] {xor} Arquitectura de protección: red local (LAN)	T	4	L3	L3	L3
[IP.4.1] Filtro de paquetes IP (red)	T	3 (u)	L3	L3	L3
[IP.4.1.1] Todo el tráfico atraviesa el filtro	T	3	L3	L3	L3
[IP.4.2] Cortafuegos (control de sesión)	T	4	L3	L3	L3
[IP.4.3] Proxy (monitorización de aplicaciones)	T	4	L3	L3	L3
[IP.4.4] Router (2 puertos) + proxy	T	4			L3
[IP.4.4.1] El router separa la red externa del servidor de proxy	T	4			L3
[IP.4.4.2] Todo el tráfico atraviesa el proxy	T	4			L3
[IP.4.5] Router (3 puertos) + proxy	T	4			L3
[IP.4.5.1] El router separa el servidor de gateway de las redes interna y externa	T	4			L3
[IP.4.5.2] Todo el tráfico atraviesa el proxy	T	4			L3
[IP.4.6] 2 routers + DMZ + proxy	T	4			L3
[IP.4.6.1] Todo el tráfico atraviesa el proxy	T	3			L3
[IP.4.6.2] Se emplean productos de fabricantes diferentes	T	4			L3
[IP.4.7] Pasarela (se cambia de protocolo)	T	4 (o)			L3
[IP.4.7.1] Todo el tráfico atraviesa la pasarela	T	4			L3
[IP.4.8] Se emplean dispositivos de sentido único (diodos)	T	4 (o)			L3
[IP.4.8.1] Todo el tráfico atraviesa el diodo	T	4			L3
[IP.4.8.2] {xor} Se controla el trafico de retorno	T	4			L3
[IP.4.8.2.1] No es físicamente posible	T	4			L3
[IP.4.8.2.2] Se controla estrictamente	T	4			L3
[IP.4.9] Cortafuegos de aire (air gap o air wall)	T	4 (o)			L3
[IP.4.9.1] Todo el tráfico atraviesa el cortafuegos	T	4			L3
[IP.4.9.2] Se controla estrictamente el trafico de retorno	T	4			L3
[IP.5] {xor} Dispositivos portátiles	T	4	L3	L3	L3

[IP.5.1] Filtro de paquetes IP (red)	T	3 (u)	L3	L3	L3
[IP.5.1.1] Todo el tráfico atraviesa el filtro	T	3	L3	L3	L3
[IP.5.2] Cortafuegos (control de sesión)	T	4			L3
[IP.5.2.1] Todo el tráfico atraviesa el cortafuegos	T	4			L3
[IP.BS] Protección de los equipos de frontera	G	5	L0-L3	L2-L3	L2-L3
[IP.BS.1] Se controla el producto	G	3	L2-L3	L3	L2-L3
[IP.BS.2] Se aplican perfiles de seguridad	G	5	L2-L3	L2-L3	L2-L3
[IP.BS.3] Cuando un equipo portatil se conecta en remoto:	G	3	L0-L1	L2	L3
[IP.BS.3.1] Se verifica la actualidad de sus componentes (parches software)	G	3	L1	L2	L3
[IP.BS.3.2] Se verifica su configuración de seguridad	G	3	L0	L2	L3
[IP.BS.4] Administración	G	3	L1-L2	L2-L3	L2-L3
[IP.BS.5] Se establece un plan de contingencia específico	T	1	L0	L2	L2
[IP.BS.6] Se emplean productos certificados o acreditados	T	3	L3	L3	L3

[MP] Protección de los Soportes de Información

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[MP.1] Se dispone de normativa relativa a soportes de información	G	2	L0	L2	L2
[MP.2] Se dispone de procedimientos relativos a soportes de información	G	2	L0	L2	L2
[MP.3] Se dispone de un inventario de soportes	G	3	L0	L2	L3
[MP.4] Gestión de soportes	G	5	L0-L2	L2-L3	L2-L3
[MP.4.1] Manejo	G	5	L0-L2	L2-L3	L2-L3
[MP.4.2] Etiquetado	G	3	L0	L2	L3
[MP.4.3] Transporte de soportes	F	4	L0	L2	L2-L3
[MP.4.4] Formación del personal en gestión de soportes	G	3	L0	L2	L3
[MP.5] Se controla la conexión de dispositivos removibles	F	5			L3
[MP.6] Contenedores de seguridad	F	5			L3
[MP.7] Seguridad de los soportes fuera de las instalaciones	F	4	L0-L1	L2-L3	L2-L3
[MP.7.1] Se requiere autorización previa para sacar soportes de las instalaciones	F	2	L0	L2	L2
[MP.7.2] Se identifica a las personas autorizadas	F	3	L1	L3	L3
[MP.7.3] Registro de entradas y salidas	F	4	L0	L2	L2-L3
[MP.7.4] Se dispone de normativa de uso de soportes fuera de las instalaciones	F	2	L1	L2	L2
[MP.7.5] El soporte se protege técnicamente antes de su salida	F	4	L0	L2	L3
[MP.7.6] El soporte se revisa a su regreso	F	3	L0	L2	L3
[MP.cont] Aseguramiento de la disponibilidad	T	4	L1-L3	L2-L3	L2-L3
[MP.IC] Protección criptográfica del contenido	G	6	L0-L2	L1-L3	L2-L4
[MP.IC.1] Se dispone de normativa relativa a la protección criptográfica de los contenidos	G	2	L0-L1	L2	L2
[MP.IC.2] Se han designado responsables	G	2	L0	L2	L2

[MP.IC.4] Se garantiza la integridad del contenido	G	5	L0	L2	L3
[MP.IC.5] Se firma el contenido	G	5	L0	L2	L3
[MP.IC.6] Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos	G	2	L0	L1	L2
[MP.IC.7] Se tienen en cuenta los requisitos de control de los mecanismos criptográficos (registro, contabilidad, auditoría, etc.)	G	3	L0	L1	L3
[MP.IC.8] {xor} Mecanismo de integridad	T	5	L2	L3	L3
[MP.IC.9] Mecanismo de cifrado	T	3	L0-L2	L2-L3	L3
[MP.clean] Limpieza de contenidos	G	4	L0-L2	L2	L2-L3
[MP.clean.1] Se dispone de normativa que determina qué información debe ser eliminada de forma segura	G	2	L2	L2	L2
[MP.clean.2] Se dispone de procedimientos para la limpieza de soportes	G	2	L0	L2	L2
[MP.clean.3] Se realiza una limpieza segura del contenido de todo soporte reutilizable del que se desprenda la organización	G	3	L1	L2	L3
[MP.clean.4] Se retiran todas las etiquetas y marcas	G	3	L0	L2	L3
[MP.clean.5] Mecanismo de limpieza	T	4	L0	L2	L3
[MP.end] Destrucción de soportes	G	3	L0-L2	L2	L2-L3
[MP.end.1] Se dispone de normativa que determina qué soportes deben ser destruidos de forma segura	G	2	L2	L2	L2
[MP.end.2] También se destruyen aquellos soportes de los que no puede eliminarse la información de forma segura	G	2	L0	L2	L2
[MP.end.3] Se dispone de procedimientos para la destrucción de soportes	G	2	L0	L2	L2
[MP.end.4] Se controla el acceso a los soportes que van a ser eliminados	T	3	L0	L2	L3
[MP.end.5] Se mantiene un registro de soportes destruidos	G	2	L0	L2	L2
[MP.end.6] Mecanismo de destrucción	T	3	L0	L2	L3

[AUX] Elementos Auxiliares

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[AUX.1] Se dispone de un inventario de equipamiento auxiliar	G	3	L1	L2	L3
[AUX.cont] Aseguramiento de la disponibilidad	T	4	_-L3	_-L3	L3
[AUX.cont.1] Se siguen las recomendaciones del fabricante o proveedor	T	4	L3	L3	L3
[AUX.cont.2] Continuidad de operaciones	T	4			L3
[AUX.start] Instalación	F	4			L3
[AUX.power] Suministro eléctrico	F	5	L0-L3	L0-L3	L2-L3
[AUX.power.1] Se dimensiona el sistema considerando necesidades futuras	F	3	L3	L3	L3
[AUX.power.2] Instalación de acuerdo a la normativa vigente	F	2	L2	L2	L2
[AUX.power.3] Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas	F	4	L2	L3	L3
[AUX.power.4] Interruptor general de la alimentación del	F	3	L2	L3	L3

sistema situado en la entrada de cada área					
[AUX.power.5] Interruptores etiquetados y protegidos frente a activaciones accidentales	F	3	L2	L3	L3
[AUX.power.6] Alimentación de respaldo	F	5	L0-L3	L0-L3	L2-L3
[AUX.AC] Climatización	F	4	L3	L3	L2-L3
[AUX.wires] Protección del cableado	F	6	L1-L3	L2-L3	L2-L4
[AUX.7] Se disponen medidas frente a posibles robos	G	5	L2	L3	L3
[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos	F	4			L3

[L] Protección de las Instalaciones

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[L.1] Se dispone de normativa de seguridad	F	2	L0	L1	L2
[L.2] Se dispone de un inventario de instalaciones	F	4	L1-L3	L2-L3	L2-L3
[L.3] Entrada en servicio	F	4	_-L1	_-L2	L2-L3
[L.3.1] Se dispone de normativa de entrada en servicio	F	2			L2
[L.3.2] Se requiere autorización previa	F	2	L1	L2	L2
[L.3.3] Se han determinado las acreditaciones o certificaciones pertinentes	F	4			L3
[L.3.4] Se requiere haber pasado las inspecciones o acreditaciones establecidas	F	3			L3
[L.3.5] Plan de Protección	F	3			L2-L3
[L.3.5.1] Se dispone de un Plan de Acondicionamiento	F	3			L3
[L.3.5.2] Se dispone de un Plan de Seguridad	F	3			L3
[L.3.5.3] Plan de Emergencia	F	3			L2-L3
[L.3.5.3.1] Plan de Evacuación	F	3			L2-L3
[L.3.5.3.2] Plan de Comunicación	F	3			L3
[L.3.5.3.3] Acceso físico a las instalaciones en caso de emergencia	F	3			L2-L3
[L.design] Diseño	F	5	L0-L3	L1-L3	L3
[L.design.1] El diseño atiende a las reglas y normas relevantes sobre salud y sanidad	F	3	L3	L3	L3
[L.design.2] El número de entradas se reduce al mínimo necesario	F	4	L2	L2	L3
[L.design.3] {xor} Puertas de acceso	F	4	L2	L3	L3
[L.design.4] Ventanas	F	4	L2	L3	L3
[L.design.5] Se dispone de protección en los conductos y aberturas (falso techo, conductos de aire, etc.)	F	3	L1	L2	L3
[L.design.6] Aislamiento acústico de las zonas en las que se hable de información confidencial	F	4 (o)	L0	L1	L3
[L.design.7] Hay una separación entre áreas de seguridad y de acceso público	F	5	L1	L2	L3
[L.design.8] Los equipos sensibles se instalan en áreas separadas	F	5	L3	L3	L3
[L.design.9] Se encuentran separadas las áreas gestionadas por otros	F	5	L1	L2	L3
[L.design.a] Se encuentran separadas las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura,	F	4	L3	L3	L3

depósitos de combustible, etc.)					
[L.design.b] Se encuentran separados los accesos para personas y vehículos	F	5	L3	L3	L3
[L.design.d] Las instalaciones son discretas minimizando indicaciones sobre su propósito	F	4	L2	L2	L3
[L.depth] Defensa en profundidad	F	5			L3
[L.depth.1] El perímetro exterior previene el acceso no autorizado	F	5			L3
[L.depth.2] Los siguientes niveles detectan accesos no autorizados	F	5			L3
[L.depth.3] Los diferentes niveles retardan el ataque	F	5			L3
[L.depth.4] El tiempo de reacción a un ataque es inferior al tiempo requerido por el atacante	F	5			L3
[L.6] {xor} public={L.IA}Mecanismo de autenticación	T	5			L2-L3
[L.6.1] Clave (PIN)	T	5			L2-L3
[L.6.2] Tarjeta (token)	T	4			L3
[L.6.3] Tarjeta + PIN	T	5 (o)			L2-L3
[L.6.3.1] Alto que se tiene - tarjeta	T	4			L3
[L.6.3.1.1] El usuario asume la responsabilidad de la tarjeta	T	3			L3
[L.6.3.1.2] Difícil de clonar	T	4			L3
[L.6.3.1.3] Cuando no se emplea, la tarjeta se guarda en lugar separado seguro	T	4			L3
[L.6.3.2] Clave (PIN)	T	4			L2-L3
[L.6.3.2.1] Se seleccionan claves fáciles de recordar pero de difícil conjetura	T	4			L3
[L.6.3.2.1.1] {xor} Tienen una cierta longitud mínima	T	4			L3
[L.6.3.2.1.1.1] 4 caracteres	T	3 (u)			L3
[L.6.3.2.1.1.2] 6 caracteres	T	4			L3
[L.6.3.2.1.1.3] 8 caracteres	T	4			L3
[L.6.3.2.1.2] No coinciden con el identificador de usuario, con nombres o fechas de nacimiento	T	3			L3
[L.6.3.2.1.3] No contienen caracteres iguales consecutivos	T	3			L3
[L.6.3.2.1.4] No son fácilmente vulnerables por ataques de diccionario	T	3			L3
[L.6.3.2.2] Los usuarios se responsabilizan de la confidencialidad de las claves	T	3			L3
[L.6.3.2.2.1] no se comparten	T	3			L3
[L.6.3.2.2.2] no se apuntan en papel (salvo que estén codificadas)	T	3			L3
[L.6.3.2.2.3] no se guardan en ficheros (salvo ficheros cifrados)	T	3			L3
[L.6.3.2.2.4] no se guardan en PDAs (excepto con una protección de acceso sólida)	T	3			L3
[L.6.3.2.3] No se utiliza la misma clave en diferentes	T	3			L3

sitios					
[L.6.3.2.4] Se emplean diferentes claves para uso privado y para desarrollar las funciones en la organización	T	3			L3
[L.6.3.2.5] {xor} La claves tiene una duración limitada	T	2			L2
[L.6.3.2.5.1] inferior a 1 año	T	2 (u)			L2
[L.6.3.2.5.2] inferior a 6 meses (180 días)	T	2			L2
[L.6.3.2.5.3] inferior a 3 meses (90 días)	T	2 (o)			L2
[L.6.3.2.5.4] inferior a 1 mes (30 días)	T	2 (o)			L2
[L.6.3.2.6] Las claves iniciales son temporales con una duración máxima limitada	T	3			L3
[L.6.3.2.7] Se cifran las claves almacenadas en el sistema	T	3			L3
[L.6.3.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5			L3
[L.6.4] Algo que se es - biometría	T	4			L3
[L.6.4.1] {xor} Mecanismo	T	4			L3
[L.6.4.2] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	4			L3
[L.6.5] Tarjeta + biometría	T	5 (o)			L3
[L.6.5.1] Alto que se tiene - tarjeta	T	4			L3
[L.6.5.1.1] El usuario asume la responsabilidad de la tarjeta	T	3			L3
[L.6.5.1.2] Difícil de clonar	T	4			L3
[L.6.5.1.3] Cuando no se emplea, el token se guarda en lugar separado seguro	T	4			L3
[L.6.5.2] {xor} Biometría	T	4			L3
[L.6.5.2.1] Huella dactilar	T	4			L3
[L.6.5.2.2] Geometría de la mano	T	3			L3
[L.6.5.2.3] Iris	T	3			L3
[L.6.5.2.4] Retina	T	3			L3
[L.6.5.2.5] Tecleo	T	3			L3
[L.6.5.2.6] Voz	T	3			L3
[L.6.5.2.7] Texto manuscrito	T	3			L3
[L.6.5.2.8] Otros ...	T	3			L3
[L.6.5.3] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello	T	5			L3
[L.AC] Control de los accesos físicos	F	7	L0-L3	L1-L3	L2-L4
[L.AC.1] El acceso tiene que ser a través de un área de recepción	F	3	L2	L3	L3
[L.AC.2] Control de los accesos	F	4	L0	L1-L2	L2-L3
[L.AC.2.1] Se dispone de normativa de control de accesos	F	2	L0	L2	L2
[L.AC.2.2] Se dispone de procedimientos para el control de accesos	F	2	L0	L2	L2

[L.AC.2.3] Se definen y documentan las autorizaciones de acceso	G	2	L0	L2	L2
[L.AC.2.4] La autorización para acceder se verifica antes de conceder el acceso	F	3	L0	L2	L3
[L.AC.2.5] Se mantiene un registro de los accesos	F	3	L0	L2	L3
[L.AC.2.6] El registro de accesos se revisa periódicamente	F	4	L0	L2	L3
[L.AC.2.7] Se investiga cualquier sospecha o intento de acceso físico no autorizado	F	2	L0	L2	L2
[L.AC.2.8] Los admitidos están acompañados permanentemente (escoltas) según política	F	4	L0	L2	L3
[L.AC.2.9] Se realiza un registro (examen minucioso) a la entrada	F	4	L0	L1	L3
[L.AC.2.a] Se realiza un registro (examen minucioso) a la salida	F	4	L0	L1	L3
[L.AC.2.b] Sistema automático de control de accesos	F	4	L0	L2	L3
[L.AC.2.c] Se dispone de un sistema de cámaras de vigilancia	F	2 (o)	L0	L2	L2
[L.AC.2.d] Los procedimientos de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones	F	3	L0	L2	L3
[L.AC.3] Control de las visitas	F	5	L0-L1	L1-L2	L2-L3
[L.AC.4] Pases o identificadores	F	5	L0	L2	L3
[L.AC.5] Los accesos permanecen cerrados fuera de las horas de trabajo	F	5	L2	L3	L3
[L.AC.6] Las áreas de trabajo se cierran y controlan periódicamente cuando están vacías	F	3	L3	L3	L3
[L.AC.8] Las salidas de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones	F	3	L2	L3	L3
[L.AC.9] Se exige que los puestos de trabajo están despejados	F	3	L0	L2	L3
[L.AC.a] Se evita el trabajo no supervisado	F	4 (o)	L0	L2	L3
[L.AC.b] Se prohíben equipos de registro (fotografía, video, audio, telefonía, etc.) salvo autorización especial	F	4	L0	L1	L3
[L.AC.c] Control de llaves, combinaciones o dispositivos de seguridad	F	4	L0-L3	L2-L3	L2-L3
[L.AC.c.1] Se dispone de un inventario	F	3	L1	L3	L2-L3
[L.AC.c.2] Las áreas de seguridad disponen de algún tipo de llave, combinación o dispositivo de seguridad para acceder a las mismas	F	4	L1	L2	L3
[L.AC.c.3] Solamente el personal autorizado puede usarlos	F	3	L2	L3	L3
[L.AC.c.4] Se custodian de forma segura, incluidos los duplicados	F	4	L3	L3	L3
[L.AC.c.5] Las llaves se cambian cuando se hayan comprometido o exista sospecha de ello	F	4	L2	L3	L3
[L.AC.c.6] Las combinaciones se cambian o modifican cuando han sido comprometidas o exista	F	4	L2	L3	L3

sospecha de ello					
[L.AC.c.7] Las combinaciones se cambian o modifican cuando haya cambios de personal que haya tenido acceso a las mismas	F	3	L2	L3	L3
[L.AC.c.8] Las combinaciones se cambian o modifican al menos cada seis meses	F	3	L0	L2	L3
[L.AC.c.9] Periódicamente, se realiza un auditoría	F	3	L0	L2	L3
[L.8] Protección del perímetro	F	4	L2	L2	L3
[L.8.1] El perímetro está claramente definido con una valla, muro o similar	F	4	L2	L2	L3
[L.8.2] {xor} La construcción es resitente frente a ataques de fuerza bruta	F	4	L2	L2	L3
[L.8.3] Se dispone de un sistema de detección de intrusión perimetral	F	4	L2	L2	L3
[L.8.4] Se dispone de cámaras de vídeo de vigilancia	F	4	L2	L2	L3
[L.8.5] El personal está concienciado y recibe formación en lo relativo a detección y reacción frente actividades sospechosas en las cercanías del recinto	F	3	L2	L2	L3
[L.9] Vigilancia	F	5			L2-L3
[L.a] Iluminación de seguridad	F	4			L3
[L.b] Protección frente a desastres	F	6	L0-L3	L1-L3	L2-L4
[L.b.1] La iluminación de emergencia cubre todas las áreas necesarias para garantizar la continuidad de las misiones críticas	F	5	L2	L3	L3
[L.b.2] Protección frente a incendios	F	6	L0-L3	L1-L3	L2-L4
[L.b.3] Protección frente a inundaciones	F	6	L0-L3	L1-L3	L3
[L.b.4] Protección frente a accidentes naturales e industriales	F	5	L0-L1	L1-L2	L3
[L.b.7] Protección frente a explosivos	F	5	L0	L1	L3
[L.b.8] Seguros	F	4	L3	L3	L3
[L.cont] Continuidad de operaciones	F	5	L1-L3	L2-L3	L3
[L.cont.1] Se analizan las implicaciones para la continuidad del negocio	F	4	L1	L2	L3
[L.cont.2] Se establece un protocolo de actuación en caso de contingencia	F	4	L1	L2	L3
[L.cont.3] Se dispone de instalaciones alternativas	F	5	L3	L3	L3
[L.cont.4] Las instalaciones alternativas están sujetas a las mismas garantías de protección que las habituales	F	4	L3	L3	L3
[L.end] Desmantelamiento	F	2			L2

[PS] Gestión del Personal

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)	P	3	L0	L2	L3
[PS.2] Se dispone de procedimientos para la gestión de personal (en materia de seguridad)	P	3			L3
[PS.3] Relación de personal	P	3	L1-L3	L2-L3	L3
[H.ST] Segregación de tareas	T	5	L0-L3	L2-L3	L2-L3

[H.ST.1] Todos los procesos críticos requieren al menos 2 personas	T	5	L1	L2	L3
[H.ST.2] Se definen roles con autorización exclusiva para realizar tareas	T	4	L0-L3	L2-L3	L2-L3
[H.ST.3] Se controla la efectividad de la estructura de segregación	T	4	L0-L3	L2-L3	L3
[PS.5] Puestos de trabajo	P	3	L0-L2	L1-L3	L2-L3
[PS.5.1] Se dispone de un inventario de puestos de trabajo	P	2	L2	L2	L2
[PS.5.2] Se especifican las funciones de los puestos de trabajo	P	2	L1	L1	L2
[PS.5.3] Se han determinado las responsabilidades en materia de seguridad de los puestos de trabajo	P	3	L0	L1	L3
[PS.5.4] Se tienen en cuenta los requisitos de seguridad de los puestos de trabajo	P	3	L0	L1	L3
[PS.5.5] Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo	P	3	L0-L2	L2-L3	L2-L3
[PS.5.6] Se mide el desempeño efectivo, en materia de seguridad, del personal asignado al puesto	P	3	L0	L1	L3
[PS.5.7] Se revisa periódicamente la especificación del puesto	P	2	L0	L1	L2
[PS.6] Contratación	P	5	_-L3	_-L3	L2-L3
[PS.6.1] Se dispone de normativa para la contratación de personal	P	3			L3
[PS.6.2] Se dispone de procedimientos para la contratación de personal	P	3			L3
[PS.6.3] Selección de personal	P	4	L0-L1	L1-L2	L3
[PS.6.4] Términos y condiciones de la relación laboral	P	3	L1-L3	L2-L3	L2-L3
[PS.6.4.1] Inclusión del ámbito, el alcance y el periodo de las responsabilidades en materia de seguridad	P	2	L1	L2	L2
[PS.6.4.2] Inclusión de obligaciones y derechos legales de ambas partes	P	2	L2	L2	L2
[PS.6.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente	P	2	L2	L2	L2
[PS.6.4.4] Acuerdos de confidencialidad	P	3	L1	L2-L3	L2-L3
[PS.6.4.5] Procedimiento disciplinario	P	3	L1-L3	L2-L3	L2-L3
[PS.6.5] Finalización de la relación laboral	P	5	L0-L2	L1-L3	L2-L3
[PS.7] Cambio de puesto de trabajo	P	3	L1	L2-L3	L3
[PS.AT] Formación y concienciación	P	3	L0-L2	L1-L2	L2-L3
[PS.9] Procedimientos de prevención y reacción	P	6	L0-L2	L2	L2-L4
[PS.9.1] frente a software dañino	P	4	L2	L2	L2-L3
[PS.9.1.1] virus	P	4	L2	L2	L3
[PS.9.1.2] spam	P	2	L2	L2	L2
[PS.9.1.3] otros ...	P	2	L2	L2	L2
[PS.a] Protección del usuario frente a coacciones	P	5			L3
[PS.cont] Aseguramiento de la disponibilidad	P	4	L0	L0-L1	L2-L3
[PS.cont.1] Se prevé suficiente holgura en el dimensionamiento de los equipos de trabajo	P	3	L0	L1	L3
[PS.cont.2] Se monitorizan continuamente los incidentes de disponibilidad de personal	P	3	L0	L1	L3

[PS.cont.3] Redundancia	P	4	L0	L0	L2-L3
[PS.cont.4] El personal alternativo está sujeto a las mismas garantías de seguridad que el habitual	P	2	L0	L0	L2
[PS.c] Personal subcontratado	P	4			L3

[H.IR] Gestión de incidentes

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[H.IR.1] Se dispone de normativa de actuación para la gestión de incidentes	G	2	L1	L2	L2
[H.IR.2] Se dispone de procedimientos para la gestión de incidentes	G	5	L0-L2	L1-L3	L2-L3
[H.IR.2.1] Actuación frente a código dañino	G	5	L0-L2	L2-L3	L2-L3
[H.IR.2.2] Actuación frente a ataques de denegación de servicio (DoS)	G	3	L1	L2	L3
[H.IR.2.3] Actuación ante fallos del sistema e interrupciones del servicio	G	3	L1	L2	L3
[H.IR.2.4] Actuación ante errores que resulten de datos del negocio inexactos o incompletos	G	4	L1	L2	L3
[H.IR.2.5] Actuación frente a violaciones de la confidencialidad	G	4	L1	L2	L3
[H.IR.2.6] Actuación frente a alarmas de los sistemas de detección de intrusión	G	3	L1	L3	L3
[H.IR.2.7] Actuación frente a alarmas de los sistemas de prevención de intrusión	G	3	L2	L3	L3
[H.IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros	G	3	L0	L1	L3
[H.IR.2.9] Actuación frente a alarmas de uso no autorizado del sistema	G	3	L1	L3	L3
[H.IR.2.a] Actuación frente a fallos del software	G	4	L1	L2	L3
[H.IR.2.b] Actuación frente a estaciones base wifi no auorizadas	G	3	L0	L2	L3
[H.IR.2.c] Detección y reacción frente a actividades de espionaje industrial	G	3	L0	L2	L3
[H.IR.2.d] Detección y reacción frente a actividades de robo de datos de carácter personal	G	3	L1	L3	L3
[H.IR.2.e] Actuación frente a otros incidentes	G	3	L2	L3	L3
[H.IR.2.f] Coordinación con otros sistemas de información afectados	G	3	L1	L2	L3
[H.IR.3] El personal designado cubre las 24h los 7 días de la semana	G	3	L2	L2	L3
[H.IR.4] El fallo del sistema deja a este en un estado controlado	G	5	L2	L3	L3
[H.IR.5] Gestión del incidente	G	5	L0-L3	L1-L3	L2-L3
[H.IR.5.1] Se suspenden cautelarmente los trabajos en el sistema afectado	G	5	L3	L3	L3
[H.IR.5.2] Se identifica y analiza la causa	G	2	L2	L2	L2
[H.IR.5.3] Se analiza el impacto del incidente	G	3	L1	L2	L2-L3
[H.IR.5.4] Se planifica la implantación de medidas	G	2	L1	L2	L2

correctoras					
[H.IR.5.5] Hay comunicación con los afectados por el incidente	G	4	L2-L3	L3	L3
[H.IR.5.6] Hay comunicación con los implicados en la recuperación del incidente	G	3	L2-L3	L2-L3	L3
[H.IR.5.7] Se informa de las acciones a la autoridad respectiva de la organización	G	2	L2	L2	L2
[H.IR.5.8] Evidencias	G	3	L0-L1	L1-L2	L3
[H.IR.6] Ayuda a los afectados	G	3	L2	L3	L3
[H.IR.7] Cooperación con otras organizaciones	G	4	L2-L3	L3	L3
[H.IR.8] Comunicación de los incidentes de seguridad	G	3	L2-L3	L3	L3
[H.IR.9] Comunicación de las deficiencias de seguridad	G	2	L2	L2	L2
[H.IR.a] Comunicación de los fallos del software	G	3	L1	L2	L3
[H.IR.b] Se dispone de un registro de incidentes	G	3	L3	L3	L3
[H.IR.c] Los fallos y las medidas correctoras se registran y se revisan	G	3	L0-L1	L2-L3	L2-L3
[H.IR.d] Control formal del proceso de recuperación ante el incidente	G	3	L0-L1	L1-L2	L2-L3
[H.IR.e] Formación y concienciación	P	3	L0-L1	L1-L2	L2-L3
[H.IR.e.1] Concienciación en la detección y reporte de incidentes	P	2	L1	L2	L2
[H.IR.e.2] Formación del personal en detección y gestión de incidentes	P	2	L1	L2	L2
[H.IR.e.3] Se tiene en cuenta la singularidad del sistema	P	3	L1	L2	L2-L3
[H.IR.e.3.1] Requisitos de seguridad	P	2	L1	L2	L2
[H.IR.e.3.2] Responsabilidades legales y contractuales	P	2	L1	L2	L2
[H.IR.e.3.3] Amenazas potenciales	P	2	L1	L2	L2
[H.IR.e.3.4] Vulnerabilidades identificadas	P	2	L1	L2	L2
[H.IR.e.3.5] Incidentes ocurridos	P	3	L1	L2	L3
[H.IR.e.4] Se prueban regularmente los procedimientos de gestión de incidentes	P	2	L0	L1	L2
[H.IR.f] Se aprende de los incidentes	G	3	L0-L1	L1-L2	L2-L3
[H.IR.g] Se toman medidas para prevenir la repetición	G	4	L2	L3	L3

[BC] Continuidad del negocio

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[BC.1] Se dispone de normativa relativa a la continuidad del negocio	G	3	L0	L1-L2	L2-L3
[BC.2] El inventario se actualiza regularmente	G	2	L0	L1	L2
[BC.BIA] Se ha realizado un análisis de impacto (BIA)	G	2	L0	L1	L2
[BC.4] Actividades preparatorias	G	3	_-L1	_-L2	L3
[BC.5] Reacción (gestión de crisis)	G	3	_-L0	_-L2	L2-L3
[BC.DRP] Plan de Recuperación de Desastres (DRP)	G	5	L0-L3	L0-L3	L2-L3
[BC.DRP.1] Se han designado responsables	G	2	L1	L2	L2
[BC.DRP.2] Todas las áreas de la organización están coordinadas	G	4	L0	L2	L3
[BC.DRP.3] Documentación	G	2	L0	L1-L2	L2
[BC.DRP.4] Notificación y activación	G	2	L0	L1	L2

[BC.DRP.5] Se dispone de un plan de recuperación	T	5	L0-L3	L1-L3	L2-L3
[BC.DRP.5.1] Están detalladas las actividades de recuperación	T	2	L0	L1	L2
[BC.DRP.5.2] Están detallados los procedimientos de recuperación	T	2	L0	L1	L2
[BC.DRP.5.3] Se han previsto los recursos necesarios	T	3	L0	L1	L3
[BC.DRP.5.4] Están previstas instalaciones alternativas	F	5	L2	L3	L3
[BC.DRP.5.5] Las copias de seguridad (backup) se realizan con la frecuencia acordada	T	5	L3	L3	L3
[BC.DRP.5.6] Están previstos los medios alternativos de almacenamiento de la información	T	5	L2	L2	L3
[BC.DRP.5.7] Están previstos los medios alternativos de procesamiento de la información	T	5	L2	L2	L3
[BC.DRP.5.8] Están previstos medios alternativos de comunicación	T	5	L0	L2	L3
[BC.DRP.5.9] Está previsto personal alternativo	P	5	L0	L1	L3
[BC.DRP.5.a] Están previstos los lugares alternativos de trabajo	F	5	L0	L1	L3
[BC.DRP.6] Se ejecuta un plan de formación	G	2	L0	L1	L2
[BC.DRP.7] Los planes se prueban regularmente	G	4	L0	L0-L1	L3
[BC.7] Restitución (retorno a condiciones normales de trabajo)	T	2	L0	L1-L2	L2

[G] Organización

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[G.1] Organización interna	G	6	_-L3	_-L3	L2-L4
[G.1.2] Comité de seguridad de la información	G	2	L2	L2	L2
[G.1.3] Coordinación interna	G	2	L1-L2	L2	L2
[G.1.4] Roles identificados	G	3	L2-L3	L2-L3	L2-L3
[G.1.5] Asignación de responsabilidades para la seguridad de la información	G	2	L1-L2	L2	L2
[G.1.6] Se dispone de asesoramiento especializado en seguridad	G	2	L1	L2	L2
[G.2] Documentación técnica (componentes)	G	3	L1-L2	L2-L3	L2-L3
[G.2.1] Documentación de los componentes del sistema	G	2	L1-L2	L2	L2
[G.2.1.1] Documentación de las instalaciones	G	2	L2	L2	L2
[G.2.1.2] Documentación de las comunicaciones	G	2	L2	L2	L2
[G.2.1.3] Puntos de interconexión (entre zonas de confianza)	G	2	L2	L2	L2
[G.2.1.4] Documentación de los puntos de acceso lógico al sistema	G	2	L1	L2	L2
[G.2.1.5] Documentación del control de acceso	G	2	L1	L2	L2
[G.2.2] Criterios de aceptación para versiones o sistemas nuevos	G	2	L1-L2	L2	L2
[G.2.3] Seguridad de la documentación del sistema	G	3	L1-L2	L2-L3	L2-L3
[G.3] Documentación organizativa (normas y procedimientos)	G	3	_-L3	_-L3	L2-L3
[G.3.1] Marco de referencia	G	2	L2	L2	L2

[G.3.2] Política de Seguridad de la Organización	G	3	L1-L3	L2-L3	L2-L3
[G.3.3] Normas de seguridad	G	2	L1-L2	L2	L2
[G.3.4] Procedimientos operativos de seguridad (POS)	G	2	_-L2	_-L2	L2
[G.3.5] Se revisa periódicamente el cumplimiento por parte del personal	G	2	L2	L2	L2
[RM] Gestión de riesgos	G	3			L2-L3
[RM.1] Se dispone de normativa en materia de gestión de riesgos	G	3			L2-L3
[RM.2] Se han designado responsables	G	3			L3
[RM.3] Se dispone de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos	G	3			L3
[RM.4] Activos	G	3			L3
[RM.5] Amenazas	G	3			L3
[RM.6] Salvaguardas	G	3			L3
[RM.7] Evaluación de riesgos	G	3			L3
[RM.8] Se revisa periódicamente	G	3			L3
[G.plan] Planificación de la seguridad	G	6	_-L2	_-L2	L2-L4
[G.plan.1] Se dispone de normativa de planificación (de seguridad)	G	2			L2
[G.plan.2] Procedimientos de planificación (de seguridad)	G	2			L2
[G.plan.3] Planificación de capacidades	G	3	L0-L2	L1-L2	L2-L3
[G.plan.4] Componentes críticos: carentes de suministradores alternativos	G	2			L2
[G.plan.5] Planificación de actividades de seguridad	G	6			L2-L4
[G.exam] Inspecciones de seguridad	G	5	L0-L1	L1-L3	L2-L3

[E] Relaciones Externas

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[E.1] Acuerdos para intercambio de información y software	G	5	L1-L2	L1-L3	L2-L3

[NEW] Adquisición / desarrollo

salvaguarda	**A**	**R**	**[actual]**	**[objetivo]**	**[PILAR]**
[NEW.S] Servicios: Adquisición o desarrollo	G	2	_-L2	_-L2	L2
[NEW.S.1] Se asignan recursos suficientes	G	1			L2
[NEW.S.2] Se establecen previamente los requisitos funcionales	G	2			L2
[NEW.S.3] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	G	2	L1-L2	L2	L2
[NEW.S.4] Se identifican los requisitos técnicos de seguridad	G	2	L1-L2	L2	L2
[NEW.SW] Aplicaciones: Adquisición o desarrollo	G	4	_-L3	_-L3	L2-L3
[NEW.SW.1] Se establecen previamente los requisitos funcionales	G	2	L1	L2	L2
[NEW.SW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	G	2	L1	L2	L2
[NEW.SW.3] Se identifican los requisitos técnicos de	G	3	L0-L2	L2	L2-L3

seguridad					
[NEW.SW.4] Adquisición de aplicaciones SW	G	3	L1-L2	L2	L2-L3
[NEW.SW.5] Desarrollo	G	4	L0-L3	L0-L3	L2-L3
[NEW.SW.5.1] Metodología de desarrollo	G	3	L0-L2	L1-L3	L3
[NEW.SW.5.1.1] Se tiene en cuenta la seguridad durante todo el ciclo de desarrollo	G	3	L1	L2	L3
[NEW.SW.5.1.2] Se tratan específicamente los datos de prueba	G	3	L2	L3	L3
[NEW.SW.5.1.3] Se contempla la posibilidad de inspeccionar el código fuente	G	3	L0	L1	L3
[NEW.SW.5.2] Los desarrolladores cambian regularmente de asignaciones	G	3	L0	L0	L3
[NEW.SW.5.3] Código fuente	G	4	L0-L2	L1-L3	L2-L3
[NEW.SW.5.4] Entorno de desarrollo	G	4	L0-L3	L1-L3	L3
[NEW.SW.5.4.1] {xor} El entorno de desarrollo está separado del de producción	G	4	L3	L3	L3
[NEW.SW.5.4.2] Hay una separación de funciones entre el personal que desarrolla y el personal encargado de producción	G	3	L0	L1	L3
[NEW.SW.5.4.3] Las herramientas de desarrollo no son accesibles al personal de producción	G	3	L0	L1	L3
[NEW.SW.5.4.4] Se controla el acceso a las herramientas de desarrollo	G	3	L1	L2	L3
[NEW.SW.5.5] Entorno de pruebas (pre-producción)	G	4	L0-L3	L2-L3	L2-L3
[NEW.SW.5.5.1] {xor} El entorno de pre-producción está separado del de producción	G	4	L3	L3	L3
[NEW.SW.5.5.2] El entorno de pruebas simula realísticamente el entorno de producción	G	2	L2	L2	L2
[NEW.SW.5.5.3] Se emplean cuentas de usuario diferentes: pruebas y producción	G	3	L2	L3	L3
[NEW.SW.5.5.4] Se revisa la corrección y completitud de la documentación	G	2	L1	L2	L2
[NEW.SW.5.5.5] Se verifica el funcionamiento de los controles de seguridad	G	3	L0	L2	L3
[NEW.SW.5.5.6] Se verifica que el nuevo sistema no afecta negativamente a las otras funciones del sistema en el que va a operar	G	3	L2	L2	L3
[NEW.SW.5.6] {xor} Protección de los datos de prueba del sistema	G	4	L3	L3	L3
[NEW.SW.5.6.1] Las pruebas no usan datos reales	G	4	L3	L3	L3
[NEW.SW.5.6.3] Las pruebas usan datos reales	G	3	L0	L2-L3	L2-L3
[NEW.SW.5.6.3.1] Se requiere autorización previa	G	2	L0	L2	L2
[NEW.SW.5.6.3.2] Se aplica el mismo control de accesos que al sistema en producción	G	3	L0	L3	L3
[NEW.SW.5.6.3.3] Cuando termina una campaña de pruebas, la información de producción se elimina del sistema de pruebas	G	3	L0	L2	L3
[NEW.SW.5.6.3.4] Se registra el uso a efectos de auditoría	G	2	L0	L2	L2

[NEW.SW.5.7] Contratos de desarrollo SW	G	2	L0-L2	L1-L2	L2
[NEW.SW.5.8] Documentación del SW	G	2	L0-L2	L1-L2	L2
[NEW.SW.5.9] Inspección del código fuente	G	3	L0	L1	L3
[NEW.SW.6] Se prefieren aplicaciones que funcionan sobre varios sistemas operativos	G	1			L2
[NEW.HW] Equipos: Adquisición o desarrollo	G	4	_-L2	_-L2	L2-L3
[NEW.HW.1] Se establecen previamente los requisitos funcionales	G	2			L2
[NEW.HW.2] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	G	2	L1	L2	L2
[NEW.HW.3] Se identifican los requisitos técnicos de seguridad	G	2	L2	L2	L2
[NEW.HW.4] Adquisición de HW	G	3	_-L2	_-L2	L2-L3
[NEW.HW.5] Desarrollo de HW	G	4			L2-L3
[NEW.HW.5.1] Metodología de desarrollo	G	2			L2
[NEW.HW.5.2] Protocolo de pruebas	G	3			L2-L3
[NEW.HW.5.3] Desarrollo	G	4			L2-L3
[NEW.HW.6] Se tienen en cuenta las necesidades de formación	G	2			L2
[NEW.HW.7] Se tienen en cuenta las necesidades de repuestos	G	2			L2
[NEW.HW.8] Documentación del HW	G	2			L2
[NEW.HW.9] Se disponen derechos de acceso para auditar la calidad y exactitud del trabajo realizado	G	2			L2
[NEW.HW.a] La calidad y exactitud del trabajo realizado se certifica según los estándares requeridos	G	2			L2
[NEW.HW.b] Entorno de pruebas	G	4			L3
[NEW.COM] Comunicaciones: Adquisición o contratación	T	2	_-L2	_-L2	L2
[NEW.COM.1] Se establecen previamente los requisitos funcionales	T	2			L2
[NEW.COM.2] Se identifica el tipo de conexión a establecer	T	2			L2
[NEW.COM.3] Se revisan las características de la solución propuesta (sobre red pública o privada, de datos, de voz y datos, etc.)	T	2			L2
[NEW.COM.4] Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio	T	2	L1-L2	L2	L2
[NEW.COM.5] Se identifican los requisitos técnicos de seguridad	T	2	L1-L2	L2	L2
[NEW.COM.6] Se revisa la arquitectura de la red de la organización	T	2			L2
[NEW.COM.7] Se identifican los riesgos de la solución propuesta, y las salvaguardas necesarias	T	2			L2
[NEW.COM.8] La solución propuesta está completamente documentada	T	1			L2
[NEW.MP] Soportes de Información: Adquisición	G	4			L3
[NEW.C] Productos certificados o acreditados	G	4			L2-L3
[NEW.C.1] Se verifica la idoneidad para la misión encomendada	G	4			L2-L3

[NEW.C.2] Se verifica la vigencia del certificado	G	3			L3
[NEW.C.3] Se satisfacen las presunciones del producto respecto del entorno	G	3			L3

Annex IX – Altres dominis

Relació d'altres dominis que es van estudiar per si s'incorporaven a la declaració d'aplicabilitat. Tot i no incorporar-los s'adjunta la relació ja que es recomana incorporar-los progressivament en el SGSI.

A9.1. Subdomini Web Municipal

El subdomini "Web Municipal" és el lloc web on l'Ajuntament de Fita Alta ofereix informació institucional i de ciutat amb l'objectiu de donar a conèixer i promocionar Fita Alta. La web municipal es pot consultar a http://www.fitaalta.cat/

La web municipal presenta en la seva capçalera enllaços al 4 llocs web relacionats d'especial interès i mostra dues maneres diferents d'accedir a la seva informació. Es 4 llocs web d'especial interès són:

- "*Turisme i Ciutat*". Lloc web dedicat a donar a conèixer la història, l'oferta cultural i el patrimoni cultural i turístic de la ciutat.
- "*Ajuntament*". Lloc web dedicat a dinamitzar la vida política local i la participació i la comunicació entre els òrgans de govern municipals i la ciutadania.
- "*Transparència*". És una via d'accés a la web de transparència i s'explica amb més detall al subdomini Transparència.
- "*Seu electrònica i tràmits*". És una via d'accés a la Seu electrònica i s'explica amb més detall al subdomini Seu electrònica.

La web municipal també ofereix dues formes diferents de la presentada a la web municipal de consultar els seus continguts: una classificada per sectors de població i l'altra classificada per temes.

Els sectors de població considerats són:

- Infants i família
- Joves
- Dones
- Gent gra
- Nova ciutadania
- Persones amb discapacitat

Els temes considerats són:

- Comerç i consum
- Cultura
- Empresa, formació i ocupació
- Convivència
- Ensenyament
- Esports i lleure
- Habitatge
- Mobilitat i transport

- Participació i ciutadania
- Serveis socials i sanitaris
- Política lingüística
- Seguretat i prevenció
- Sostenibilitat i medi ambient
- Urbanisme i via pública

A9.2. Subdomini Transparència

El subdomini "Transparència" correspon al lloc web per a impulsar una gestió transparent de l'administració i pretén construir noves maneres de gestionar les polítiques públiques i obrir-les a la ciutadania donant compliment a la Llei 19/2014, de 29 de desembre, de transparència, accés a la informació pública i bon govern a les entitats locals.

La web municipal es pot consultar a http://transparencia.fitaalta.cat/ i es presenta la informació tant de l'Ajuntament com dels seus organismes autònoms i empreses municipals.

A9.3. Subdomini Centre de Procés de dades

El subdomini "Transparència" correspon a les instal·lacions i equipaments de procés de dades de l'Ajuntament de Fita Alta. A diferència de la resta de subdominis que són subdominis lògics el subdomini "Centre de Procés de Dades" és un domini físic. En aquest subdomini és s'apliquen de forma principal tots els objectius i controls referents a la seguretat física i ambiental, sobre els recursos humans, controls d'accessos que no són d'aplicació als dominis lògics en igual mesura.

L'Ajuntament de fita Alta té uns sistemes TIC constituïts per 2 CPD sincronitzats i ubicats en dos edificis diferents i interconnectats amb una xarxa de telecomunicacions pròpia i gestionada per tècnics municipals que abasta els 2 CPD i la resta d'edificis municipals. El serveis de telefonia corporatiu utilitzen telefonia IP i està gestionat pels tècnics de TI propis de la corporació.

També és interessant remarcar que el personal del departament de TI està ubicat físicament en un Centre Empresarial de Desenvolupament i Innovació en unes instal·lacions no corporatives. Des d'aquest centre i de forma remota és realitza la gestió de les infraestructures i serveis municipals. Aquest centre no disposa de cap CPD però conté un hub de comunicacions especial per a donar suport a la gestió dels serveis TIC.

A9.4. Subdomini Intranet

El subdomini "Transparència" correspon al lloc web de la xarxa interna de l'Ajuntament que ofereix accés a informació personal, informació corporativa i accés a les aplicacions als treballadors de l'organització. El subdomini no és accessible des d'Internet ni des de cap xarxa externa i està basat en tecnologia web. En aquests moments moments la intranet municipal es troba en procés de migració de dels seus serveis basats en servidors windows amb IIS a servidors Linux amb Apache.

Tot i que no totes les aplicacions internes corporatives són accessibles utilitzant la intranet corporativa pel fet d'utilitzar tecnologies client/servidor el subdomini intranet aglutina el 80% de les aplicacions d'ús intern corporatiu de l'Ajuntament. Aquesta proporció serà més gran en el futur proper ja que la política de desenvolupament i adquisició de programari és recolza en la utilització de tecnologia web que sigui integrable amb la intranet.

Aquest subdomini és especialment rellevant en les dimensions de confidencialitat i accessibilitat ja que en ell es gestiona la informació més compromesa de l'organització i s'utilitza com la base per al suport de la majoria de serveis que els diferents departaments municipals ofereixen a la ciutadania i les empreses.

La informació personal que s'ofereix des de la intranet és la següent:

- Informació sobre les obligacions d'ús del sistema informàtic
- Informació general, sobre la LOPD i l'ENS
- Accés al portal de l'empleat i les dades personals
- Notificació d'incidències tècniques al CAU del servei de TI
- Accés al fitxador virtual
- Accés al correu electrònic
- Gestió de treballs, incidències i quotes d'impressió

La informació corporativa està estructurada segons l'organigrama corporatiu i ofereix un espai d'aplicacions, documents, webs d'interès i estructuració de la informació en subcarpetes a tots els departament.

La informació a les aplicacions web està estructurada en 4 grans àmbits:

- Recursos Humans amb 3 aplicacions (Fitxador, Portal de l'empleat i el Directori telefònic).
- Aplicacions Generals. En aquest àmbit tenen un especial pes les aplicacions dedicades a l'Administració electrònica amb 14 aplicacions de les 26 que es poden trobar.
- Aplicacions gràfiques.
- Aplicacions departamentals. Aquest àmbit conté 29 aplicacions classificades en 9 àrees de gestió.