MÀSTER INTERUNIVERSITARI DE SEGURETAT DE LES TECNOLOGIES DE LA INFORMACIÓ I DE LA COMUNICACIÓ

PLA DIRECTOR DE SEGURETAT

AJUNTAMENT DE RIBEROLA

MEMÒRIA DESCRIPTIVA

TREBALL DE FI DE MÀSTER

Juny 2013

DIRECTOR: Carles Garrigues

CONSULTOR: Arsenio Tortajada

ALUMNE: Ricard Salvat

UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

ÍNDEX

0. RESUM / SUMMARY.....1
1. INTRODUCCIÓ 2
2. CONTEXTUALITZACIÓ.....5
2.1 Descripció de l'empresa.....5
2.2 Estructura organitzativa.....5
2.2.1 Organització política.....5
2.2.2 Departaments de l'Ajuntament.....6
2.3 Infraestructures.....7
2.4 Sistemes de la informació i comunicació.....7
2.4.1 Xarxes de comunicacions.....7
2.4.2 Centres de processament de dades.....10
2.4.3 Sistemes I aplicacions.....11
2.4.4 Estacions de treball.....12
2.5 Abast del Pla Director de Seguretat.....13
3. OBJECTIUS.....14
4. ANÀLISIS DIFERENCIAL.....16
4.1 ISO/IEC 27002 i Esquema Nacional de Seguretat.....17
4.2 Anàlisi diferencial 18
5. SISTEMA DE GESTIÓ DOCUMENTAL.....25
5.1 Política de seguretat.....25
5.2 Procediment d'auditories internes.....26
5.3 Gestió d'indicadors.....26
5.3.1 Tipus d'indicadors.....27
5.3.2 Pautes d'implantació.....28
5.4 Procediment de revisió per direcció.....29
5.5 Gestió de rols i responsabilitats.....29
5.6 Metodologia d'anàlisi de riscos.....30
5.6.1 Antecedents.....30
5.6.2 Objectius a Magerit.....31
5.6.3 Visió de conjunt.....32
5.6.4 Fases de Magerit.....33
5.6.5 Establiment de paràmetres – Valoració d'actius.....34
5.6.6 Establiment de paràmetres – Dimensions de seguretat.....34
5.6.7 Establiment de paràmetres – Valoració de vulnerabilitats.....35

5.6.8 Establiment de paràmetres – Valoració dels impactes....35
5.6.9 Establiment de paràmetres – Valoració dels controls de seguretat....36
5.6.10 Amenaces....36
5.7 Declaració d'aplicabilitat....37
6. ANÀLISI DE RISCOS....38
6.1 Inventari d'actius....38
6.2 Valoració dels actius....41
6.3 Dimensions de seguretat....41
6.4 Resum de valoració d'actius....42
6.5 Anàlisi d'amenaces i impacte potencial....50
6.6 Nivell de risc acceptable i risc residual....53
6.6.1 Instal·lacions....55
6.6.2 Dades....55
6.6.3 Claus criptogràfiques....56
6.6.4 Serveis....56
6.6.5 Aplicacions i programari....57
6.6.6 Maquinari o Hardware....58
6.6.7 Comunicacions....60
6.6.8 Suports d'informació....60
6.6.9 Equipaments auxiliars....60
6.6.10 Personal....61
6.7 Síntesi dels resultats obtinguts....61
7. PROPOSTES DE PROJECTES....67
7.1 Introducció....67
7.2 Projectes a curt termini....67
7.2.1 Adquisició de programari antivirus corporatiu 68
7.2.2 Procediments d'actualitzacions en sistemes operatius....70
7.2.3 Documentació/implantació de polítiques de seguretat....72
7.2.4 Realització de l'inventari d'actius....74
7.2.5 Millora de climatització en els centres de processament de dades....76
7.2.6 Revisió de procediments en recursos humans....78
7.3 Projectes a mig termini....80
7.3.1 Formació del personal en seguretat de les TIC....80
7.3.2 Gestió d'incidències: Programari i procediments 83
7.3.3 Definició de plans de continuïtat 85
7.3.4 Definició de procediments de còpies de seguretat....87
7.4 Projectes a llarg termini....89
7.4.1 Procediments i gestió d'auditories internes / externes....89

7.4.2 Revisió i millora de les polítiques d'active directory (domini).....90
7.4.3 Reestructuració del departament TIC.....92
7.5 Resum i conclusions.....94
7.5.1 Planificació dels projectes al llarg dels tres anys.....94
7.5.2 Estimació econòmica.....95
7.5.3 Impacte dels projectes en l'anàlisi de riscos.....96
7.5.4 Impacte dels projectes en el compliment de la ISO 27001.....97
8. AUDITORIA DE COMPLIMENT.....99
8.1 Introducció.....99
8.2 Auditoria de compliment.....100
8.3 No conformitats.....129
8.4 Observacions.....142
8.5 Presentació de resultats de l'auditoria de compliment.....145
A1. ANNEX I – DOCUMENTS DEL SISTEMA DE GESTIÓ DOCUMENTAL.....148
A1.1 Política de seguretat.....148
A1.1.1 Aprovació i entrada en vigor.....149
A1.1.2 Objectius i missió de l'ajuntament.....149
A1.1.3 Objectius i missió de la Política de Seguretat.....149
A1.1.4 Abast.....150
A1.1.5 Marc normatiu.....151
A1.1.6 Revisió de la Política de Seguretat.....151
A1.1.7 Organització de la seguretat.....151
A1.1.8 Anàlisi i gestió dels riscos.....155
A1.1.9 Desenvolupament de la política de seguretat de la informació.....156
A1.1.10 Seguretat de la informació.....158
A1.1.11 Dades de caràcter personal.....158
A1.1.12 Obligacions del personal.....159
A1.1.13 Terceres parts.....159
A1.2 Procediment d'auditories internes.....160
A1.2.1 Objectius i abast.....160
A1.2.2 Rols i responsabilitats.....160
A1.2.3 Procediment.....161
A1.2.4 Seguiment de l'auditoria i finalització 164
A1.2.5 Qualificació dels auditors.....164
A1.2.6 Registres.....165
A1.3 Fitxa d'indicador.....165
A1.4 Indicadors per objectiu de control.....166
A1.5 Procediment de revisió per direcció.....183

A1.5.1 Introducció....183
A1.5.2 Periodicitat....184
A1.5.3 Procediment....184
A1.5.4 Dades d'entrada....184
A1.5.5 Dades de sortida o resolució....185
A1.5.6 Altres consideracions....186
A1.6 Gestió de rols i responsabilitats....186
A1.6.1 Introducció....186
A1.6.2 Estructura organitzativa....187
A1.6.3 Rols....188
A1.6.4 Responsabilitats....188
A1.7 Declaració d'aplicabilitat....190
A2. ANNEX II – ANÀLISI D'AMENACES....211
A3. ANNEX III – DOCUMENTACIÓ AUDITORIA DE COMPLIMENT....239
A3.1 MODEL DE FITXA PER NO CONFORMITATS MAJORS/MENORS....239
A3.2 MODEL DE FITXA PER OBSERVACIONS....240
B. BIBLIOGRAFIA....241

0. RESUM / SUMMARY

RESUM

Aquest Treball de Fi de Màster pertany als estudis del Màster Interuniversitari de Seguretat de les Tecnologies de la Informació i Comunicació, organitzat per la Universitat Oberta de Catalunya (UOC), la Universitat Autònoma de Barcelona (UAB), la Universitat Rovira i Virgili (URV) i la Universitat de les Illes Balears (UIB).

L'objectiu del projecte és l'elaboració d'un Pla de Seguretat per una administració pública local fictícia, anomenada Ajuntament de Riberola, per tal que pugui assentar les bases d'un Sistema Gestor de Seguretat de la Informació.

El Pla de Seguretat s'emmarca dins la norma ISO 27001:2005, i els codis de bones pràctiques esmentats en la ISO 27002:2005, que estableixen les especificacions per implementar, gestionar, supervisar i millorar un Sistema Gestor de Seguretat de la Informació. S'ha realitzat un anàlisi de la situació actual de la seguretat en l'àmbit de les Tecnologies de la Informació i la Comunicació, per tal de poder definir uns objectius a curt i llarg plaç i proposar un conjunt de projectes per tal d'arribar-hi. Dins d'aquest anàlisi realitzat podem destacar l'anàlisi diferencial, l'anàlisi de riscos (utilitzant MAGERIT com a metodologia) i l'anàlisi de compliment de la ISO.

SUMMARY

This Final Work of Master belongs to Interuniversity Master of Security in Information Technology and Communications, organized by Universitat Oberta de Catalunya (UOC), Universitat Autònoma de Barcelona (UAB), Universitat Rovira i Virgili (URV) and Universitat de les Illes Balears (UIB).

The objective of the project is to create a Security Plan for a ficticious public local administration, named Ajuntament de Riberola, to lay dawn the main bases of an Information Security Management System.

This Security Plan follows the ISO 27001:2005 guidelines and ISO 27002:2005 best practices, which establish the main especifications to implement, manage, review and improve an Information Security Management System. We have made several analysis of the entity's current situation to be able to define short term and long term goals, proposing a set of projectes to improve IT organitzation's security. From all analysis, we can highlilght differential ISO analysis, risk analysis (using MAGERIT metodology) and ISO compliance analysis.

1. INTRODUCCIÓ

Actualment la informació és un dels actius més importants per la majoria d'empreses i organitzacions. Durant els últims anys, les empreses s'han anat interconnectant entre elles i oferint serveis a clients mitjançant Internet. Per tant, la seguretat de les seves dades està més exposada a possibles atacs i vulnerabilitats que poden afectar-ne la seva disponibilitat, integritat o confidencialitat.

La seguretat de la informació tracta de protegir les dades per assegurar la continuïtat del negoci o activitat diària de l'organització, minimitzant els danys i maximitzant el retorn de les inversions i les oportunitats de negoci [**ISO1**].

Per aquesta raó, s'elaborarà un **Pla Director de Seguretat** per una empresa real de la qual disposem de suficient informació, tant de la seva estructura com de l'estat actual de la seva seguretat en matèria de les Tecnologies de la Informació i la Comunicació.

Aquest pla constitueix la fulla de ruta que ha de seguir una empresa per a gestionar de forma adequada la seguretat, permetent no només conèixer-ne el seu estat, sinó els punts on l'empresa cal que actuï per tal de millorar-la. Per tant, aquest pla és un document que segueix un model de millora continua (“*PLAN-DO-CHECK-ACT*” *o* “*PLANIFICAR-FER-COMPROVAR-ACTUAR*”), definit en la ISO/IEC 27001 (*Figura 1-1*).

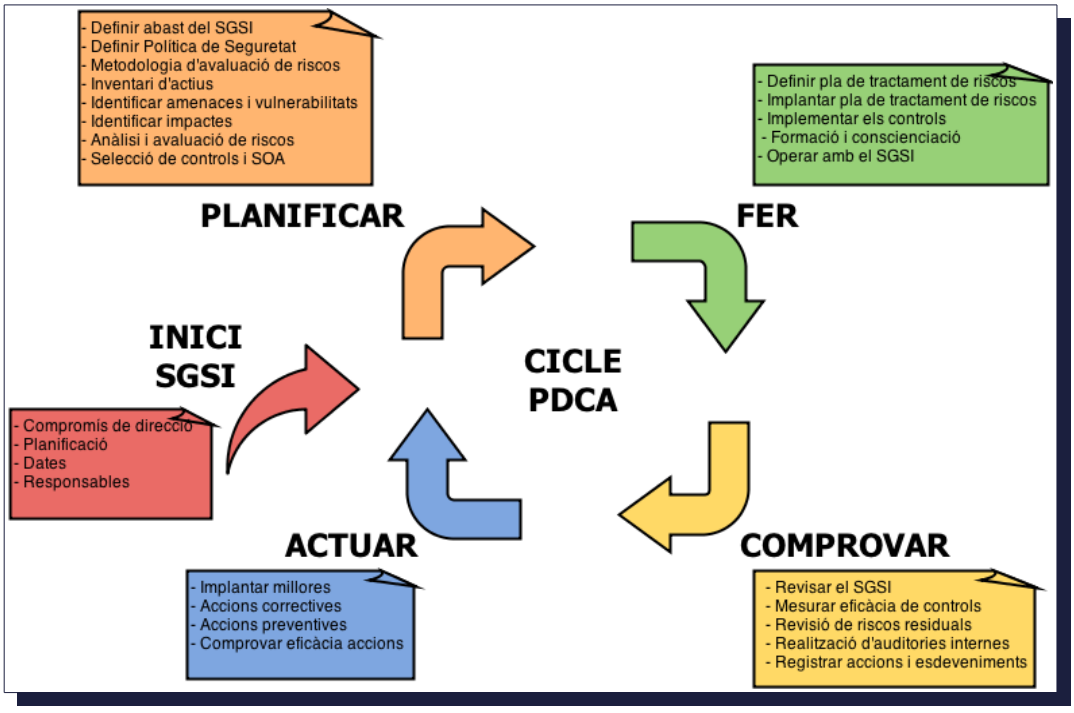

Figura 1-1: Cicle de millora continua d'un SGSI

Les bases d'aquest Pla Director de Seguretat s'aniran generant mitjançant una sèrie de fases que comprenen els següents punts:

- Analitzar i detallar l'inventari d'actius de l'empresa.
- Estudiar les amenaces a les que està exposada.
- Anàlisis de l'impacte potencial de cadascuna de les amenaces.
- Proposta d'un pla d'acció per tal de pal·liar aquestes amenaces.
- Avaluar l'impacte residual un cop aplicat el pla d'acció.

El marc legal espanyol reflecteix actualment la importància de la seguretat de la Informació mitjançant certes lleis que s'han anat creant els últims anys: Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal, Llei 34/2002 del 11 de juliol de Serveis de la Societat de la Informació i Comerç Electrònic i finalment l'**Esquema Nacional de Seguretat**, que es regula en el Real Decret 3/2010 del 8 de gener i s'estableix en l'article 42 de la llei 11/2007 del 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

L'**Esquema Nacional de Seguretat (ENS)** ve a confirmar la necessitat d'implantar Sistemes de Gestió de Seguretat de la Informació per part de les Administracions Públiques espanyoles, ja que són aquestes últimes les que es veuen afectades per l'àmbit d'actuació de l'ENS.

L'ENS persegueix els següents objectius [segons **PAEO**]:

- Crear les condicions necessàries de confiança en l'ús dels mitjans electrònics, mitjançant mesures per garantir la seguretat de la informació i els serveis electrònics, que permeti als ciutadans i a les Administracions Públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans electrònics.
- Establir una política de seguretat en l'ús de mitjans electrònics en l'àmbit de la Llei 11/2007, que estarà constituïda pels principis bàsics i requeriments mínims per una protecció adequada de la informació.
- Introduir elements comuns que han de guiar l'actuació de les Administracions Públiques en matèria de seguretat de les tecnologies de la informació i la comunicació.
- Aportar un llenguatge comú per facilitar la interacció entre Administracions Públiques, així com la comunicació dels requeriments de seguretat de la informació a la Industria.
- Proporcionar un tractament homogeni a la seguretat que faciliti la cooperació en la prestació de serveis d'administració electrònica quan participen diverses entitats.
- Facilitar un tractament continuat de la seguretat.

Per tal d'aconseguir aquests objectius s'ha decidit crear un **Pla Director de Seguretat** utilitzant com a marc estàndard de referència les **ISO/IEC 27001** (provinent de la ISO 17799) i **ISO/IEC 27002**, on es tracten requisits i codis de bones pràctiques en la gestió de la seguretat de la informació (“*Information technoloy - Security techniques - Code of pratice for information security management*”). Aquestes bones pràctiques són aptes per qualsevol tipus d'empresa o organització.

L'adaptació d'aquests estàndards facilitarà l'adaptació de l'organització a l'**Esquema Nacional de Seguretat**.

2. CONTEXTUALITZACIÓ

El projecte actual consisteix en l'elaboració d'un **Pla Director de Seguretat** per una administració pública d'àmbit local. En el present document aquesta administració s'anomenarà de manera fictícia amb el nom d'Ajuntament de Riberola.

Al tractar-se d'una administració pública, es veu afectada per l'Esquema Nacional de Seguretat, el qual pràcticament obliga a l'organització a disposar d'un Sistema de Gestió de Seguretat de la Informació.

Per tant, l'organització creu adient l'elaboració d'un Pla Director de Seguretat per tal d'adaptar-se a les exigències de seguretat actuals i per millorar la seguretat de la informació que gestiona i elabora diàriament.

2.1 DESCRIPCIÓ DE L'EMPRESA

L'Ajuntament de Riberola gestiona un municipi de prop de 13.000 habitants i un àrea d'uns 16 Km^2. Disposa de més de 200 treballadors distribuïts en diferents dependències i departaments.

2.2 ESTRUCTURA ORGANITZATIVA

L'estructura de l'Ajuntament de Riberola es pot dividir en l'organització política d'una banda i els diferents departaments de l'altra.

2.2.1 ORGANITZACIÓ POLÍTICA

El consistori està presidit per un Alcalde i un determinat nombre de regidors. Els òrgans bàsics de govern, com en qualsevol altre Ajuntament, són:

- L'alcalde o alcaldessa
- Els/les tinents d'alcalde
- Els/les regidors/es
- La Junta de Govern Local
- El Ple

Els i les tinents d'alcalde i regidors són els responsables dels diferents departaments de l'Ajuntament, on s'engloba el personal tècnic i administratiu que realitza les tasques pertinents a l'organització.

2.2.2 DEPARTAMENTS DE L'AJUNTAMENT

L'Ajuntament està dividit en departaments, cadascun dels quals realitza un conjunt de funcions concretes dins l'organització. Aquests departaments són els següents:

- Alcaldia
- Arxiu Municipal
- Cultura
- Intervenció
- Ensenyament
- Esports
- Festes
- Hisenda
- Joventut
- Medi Ambient
- Policia Municipal
- Premsa i Protocol
- Promoció Econòmica
- Oficina d'Atenció al Ciutadà (OAC)
- Oficina Tècnica
- Recursos Humans
- Rendes i Recaptació
- Secretaria
- Serveis Socials i Gent gran
- Tecnologies de la Informació i la Comunicació (2 *treballadors*)
- Tresoreria

Addicionalment als departaments, l'Ajuntament dóna serveis a altres organitzacions o empreses públiques (tractant-les funcionalment com a departaments). Entre aquestes podem destacar un museu, una empresa pública de turisme, dos mancomunitats i la biblioteca municipal.

Aquests departaments poden tenir subdivisions degut a la seva complexitat, com per exemple oficina tècnica (brigades de llum, obra, etc.) o cultura (escoles de música, arts i dansa, sales d'actes, etc.).

2.3 INFRAESTRUCTURES

Els departaments esmentats en l'apartat anterior donen serveis al ciutadà des de diferents ubicacions. Per tant, es disposen de diferents edificis i espais per tal de dotar als departaments de les infraestructures necessàries. Repartits pel municipi existeixen més de tretze espais a més de la Casa Consistorial, tots ells connectats per una anella de fibra òptica.

Per tant, no només es tracta i es gestiona informació des de la Casa Consistorial, sinó des de qualsevol dels edificis que formen part de l'organització.

2.4 SISTEMES DE LA INFORMACIÓ I COMUNICACIÓ

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

- Xarxes de comunicacions
- Centres de processament de dades
- Sistemes
- Estacions de treball

2.4.1 XARXES DE COMUNICACIONS

En aquest apartat s'engloba qualsevol xarxa de comunicacions que utilitza actualment l'Ajuntament, ja sigui internament o utilitzant algun servei extern ofert per un proveïdor. Per tant, en aquest apartat cal tenir en compte: l'**anella de fibra òptica municipal**, el **servei de telefonia i Fax** i la **xarxa d'accés a dades i Internet**. En general, el cablejat de les diferents dependències és amb Ethernet UTP categoria 5e/6. En algun cas, degut a la mida de l'edifici, també es desplega fibra òptica multimode.

2.4.1.1 Anella de fibra òptica

L'anella de fibra òptica municipal consisteix en una xarxa de fibra òptica monomode que permet la connexió de diferents edificis públics. La xarxa és propietat de l'Ajuntament de Riberola i és gestionada pel Departament de Tecnologies de la Informació i la Comunicació.

Aquesta xarxa permet centralitzar serveis a la Casa Consistorial, de manera que el

personal que treballa en les diferents localitzacions accedeix als serveis oferts des de la Casa Consistorial. Aquest punt genera un estalvi en comunicacions i infraestructura.

L'anella està implementada mitjançant tres nodes que comuniquen els diferents clients o espais. L'estructura actual es pot veure en la *Figura 2-4-1*.

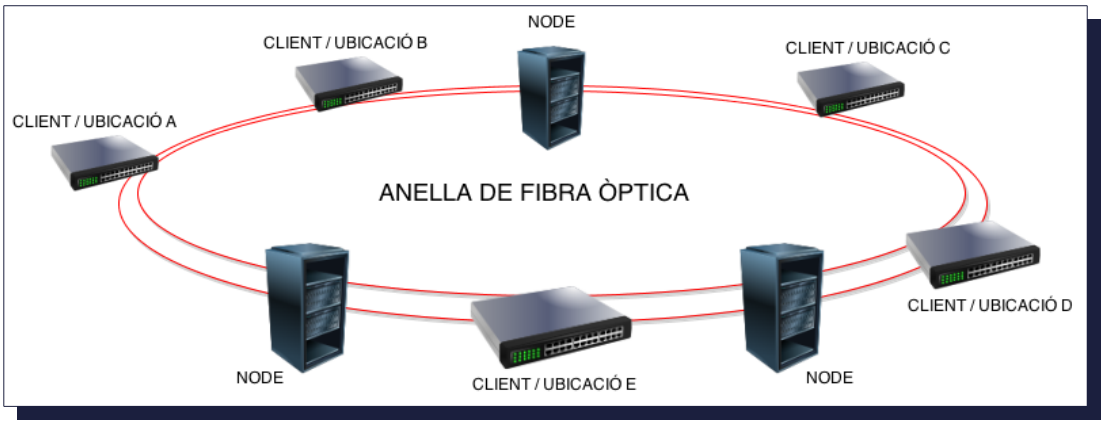

Figura 2-4-1: Estructura de l'anella de fibra òptica

Tal i com es pot observar en la *Figura 2-4-1*, els clients connecten en la major part dels casos a dos dels nodes, per tal de tenir una connexió redundant. D'aquesta manera, un tall físic de la connexió cap un node no afectaria les comunicacions perquè s'utilitzaria l'altre node. Tot i així, actualment l'anella es troba inacabada, i per tant no està tancada. Això implica que un tall en el circuit actual dels nodes si provocaria un tall a certes dependències.

El tràfic de xarxa de l'anella està segmentant (mitjançant VLAN's) per tal de dividir el tràfic en diferents xarxes independents. Aquestes són: administració de l'anella, dades, VoIP, xarxa pública i xarxa DMZ.

2.4.1.2 Servei de telefonia i Fax

El servei de telefonia es proporcionat mitjançant VoIP a totes les dependències municipals (utilitzant la infraestructura de l'anella de fibra òptica). D'aquesta manera, les diferents dependències utilitzen la centraleta IP que es troba ubicada a la Casa Consistorial. Això proporciona una disminució de costos (trucades gratuïtes entre dependències municipals i majors descomptes en contractació), així com una simplificació de la gestió per part del Departament de Tecnologies de la Informació i la Comunicació (TIC) ja que només cal administrar una sola centraleta.

Aquesta centraleta IP utilitza dues possibles sortides cap a la xarxa de telefonia exterior: un primari per orígens i destinacions de telefonia fixa i un altre primari per a telefonia mòbils. Totes les numeracions de les diferents dependències estan configurades per tal d'entrar pel primari de telefonia fixa. Entre aquestes numeracions

cal destacar el telèfon 010 d'atenció al ciutadà i els telèfons d'emergències de la Policia Municipal, especialment crítics.

Finalment, el Fax es rep a la Casa Consistorial mitjançant dos aparells de Fax, un primer que respon i digitalitza el document. I un segon aparell que respon més tard, en cas que el primer no funcioni, i que imprimeix en paper. Això també suposa un estalvi en paper i tinta, ja que molts fax són publicitat.

2.4.1.3 Xarxa d'accés a dades i Internet

La xarxa de dades i les connexions a Internet són gestionades des dels servidors ubicats a la Casa Consistorial. Mitjançant l'anella de fibra òptica, aquests serveis són accessibles a totes les dependències municipals, de manera que no cal realitzar múltiples inversions en servidors i infraestructura, ja que està tot centralitzat.

Per Internet es disposen de dues sortides, una ubicada en una seu externa (accessible per la xarxa de fibra òptica) i l'altra a la Casa Consistorial. Les dues es basen en una connexió ADSL convencional de 10 Mb i 20 Mb respectivament.

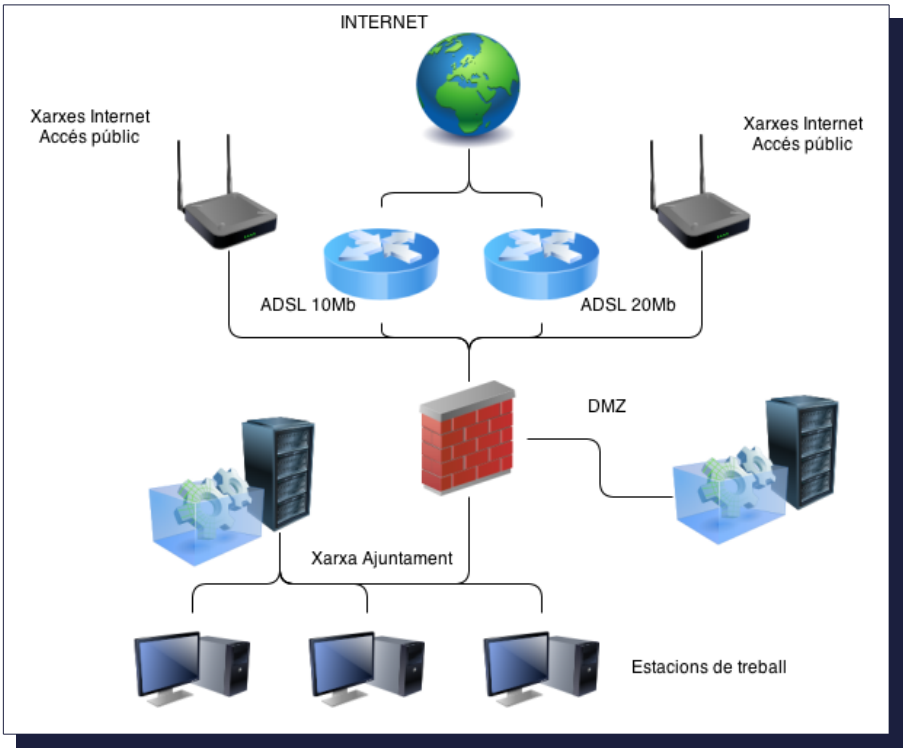

Figura 2-4-2: Diagrama bàsic de la xarxa

La xarxa de dades disposa d'un tallafocs i tres xarxes, una anomenada externa, una de pública i una zona desmilitaritzada o DMZ. El diagrama de la xarxa es pot observar en la *Figura 2-4-2*.

En la xarxa externa hi ha la sortida del tallafocs de la xarxa de l'Ajuntament, els dos

punts de connexió a Internet (en dos edificis separats) i algunes xarxes WiFi que proporcionen connexions a Internet d'accés públic.

Del tallafocs hi ha una connexió cap a una DMZ, amb polítiques d'accés més permissives on resideix el servidor de correu corporatiu.

Finalment, la xarxa privada o corporativa consisteix en els diferents servidors i les estacions de treball de les diferents dependències.

2.4.1.4 Videovigilància IP

Es disposa d'un conjunt de càmeres ubicades en diferents dependències municipals les quals realitzen gravacions en detectar moviment. Aquestes gravacions s'emmagatzemen durant un mes en un servidor ubicat al Centre de Processament de Dades de la Casa Consistorial. Després d'un mes són esborrades segons marca la Llei Orgànica de Protecció de Dades 11/2007.

2.4.2 CENTRES DE PROCESSAMENT DE DADES

L'Ajuntament de Riberola disposa de quatre centres de processament de dades (CPD), dos dels quals estan ubicats en la Casa Consistorial i els altres dos estan situats en edificis de propietat municipal, un d'ells de dimensions considerables. A continuació se'n resumeix el seu contingut:

2.4.2.1 CPD Casa Consistorial 1

Aquest CPD conté tota la electrònica de xarxa de la Casa Consistorial (tant de veu com de dades), així com un dels nodes de fibra òptica i les connexions a la xarxa de telefonia. També conté la centraleta IP que gestiona tota la telefonia (Asterisk). Disposa d'accés mitjançant porta amb clau, refrigeració amb aire condicionat i SAI (sistema d'alimentació ininterrompuda).

2.4.2.2 CPD Casa Consistorial 2

En aquest CPD estan ubicats la major part dels servidors Windows i Linux que donen servei a l'Ajuntament. De la mateixa manera que la sala anterior, també es disposa de refrigeració amb aire condicionat, SAI i accés per porta amb clau, tot i que disposa d'alguna finestra amb vidre accessible.

2.4.2.3 CPD Edifici mitjà municipal

Aquest CPD conté únicament l'electrònica de xarxa d'un dels nodes de fibra òptica. En aquest cas l'accés és per porta amb clau, però no existeix refrigeració ni SAI.

2.4.2.4 CPD Edifici municipal gran

En aquesta sala s'hi ubica un altre dels nodes de fibra òptica, un servidor de còpies de

seguretat (execució diària, sincronització de màquines virtuals) i l'electrònica de xarxa necessària per proporcionar serveis a diferents punts de l'edifici (desplegament de petits nodes connectats per fibra òptica multimode). Aquest CPD disposa d'accés per porta amb clau, refrigeració i SAI.

2.4.3 SISTEMES I APLICACIONS

Per a gestionar les aplicacions i serveis per l'organització, es disposa de diferent maquinari i sistemes heterogenis.

2.4.3.1 Sistemes

Es treballa en un entorn heterogeni de sistemes Windows i Linux, a més de disposar de certs servidors virtuals i uns altres de físics. Els usuaris i els recursos compartits en general estan gestionats amb un controlador de domini Windows. Existeixen set servidors addicionals Windows, la major part virtuals, i es disposa de nou sistemes Linux, dos d'ells virtuals, la resta físics. Els serveis que realitzen els sistemes Windows són principalment els següents:

- Servei de DNS, DHCP i Active Directory.
- Compartició de carpetes (dades departaments) i bases de dades.
- Gestió de bases de dades i publicació de serveis i pàgines en servidor web (IIS).
- Serveis d'impressió.
- Servidors d'aplicacions.
- Còpies de seguretat en cinta (servidor Windows 2003 físic).
- Sincronització d'imatges *VMWare* en ubicació remota (còpies seguretat).

D'altra banda, els diversos sistemes Linux existents ofereixen:

- Servei de pàgines web corporatives (*Apache*, *MySQL* i *PHP*).
- Execució de programes de control (*scripts*) i enviament/recepció de SMS.
- Monitorització d'elements de la xarxa (*Nagios*) i Sistema de Detecció d'Intrusions (IDS – *Alienvault OSSIM*).
- Servidor de correu corporatiu per l'Ajuntament i entitats vinculades.
- Tallafocs i *proxy* transparent.
- Servidor d'informes (*JasperReports Server*).
- Tractament de càmeres IP.

- Centraleta VoIP *Asterisk*.
- Tractament de gravacions de trucades del telèfon d'emergències.
- Allotjament web extern, servidor dedicat. Pàgina corporativa.

2.4.3.2 Aplicacions

S'utilitza programari fet per tercers (proveïdors) per les funcions més crítiques de l'Ajuntament, com són: comptabilitat, rendes i recaptació, expedients, padró i registre d'entrada i sortida. Tret d'això, des del Departament de Tecnologies de la Informació i la Comunicació s'han anat implementat petites funcionalitats i pàgines web (tret de l'oficial de l'Ajuntament, que ha estat realitzada per una empresa externa).

2.4.4 ESTACIONS DE TREBALL

Coexisteixen actualment tres sistemes operatius diferents, tot i que en diferents proporcions. D'unes 140 estacions de treball, els diferents sistemes es distribueixen entre Windows 2000, Windows XP i Windows 7 de la següent manera (*Figura 2-4-3*):

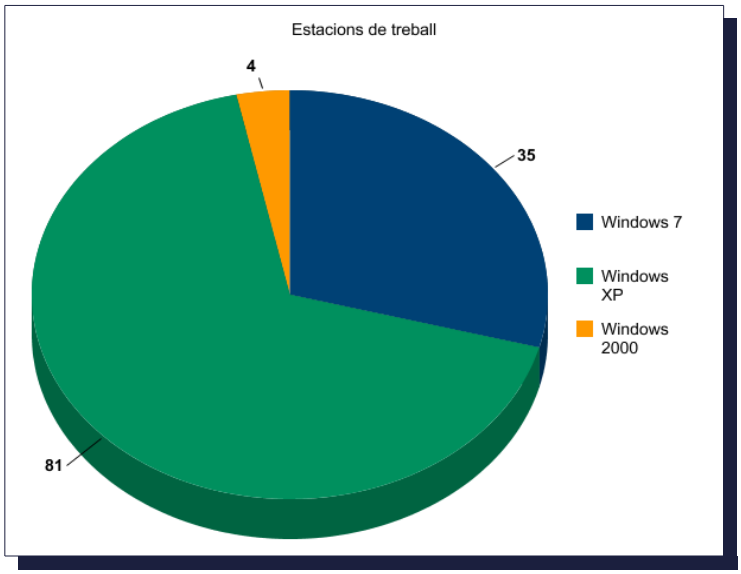

Figura 2-4-3: Distribució dels diferents sistemes de les estacions de treball

Per tant, la major part de les estacions són Windows XP. Queden 4 estacions encara amb Windows 2000 (ja no suportat per Microsoft) i Windows 7 disposa d'un percentatge proper al 30%.

Cal destacar que no es disposa d'un antivirus corporatiu sinó que les màquines en disposen d'un en local.

Els usuaris de les estacions de treball es validen en l'*Active Directory* i si les credencials són correctes s'obtenen els permisos pertinents per accedir tant al sistema com als

recursos i serveis compartits de la xarxa.

2.5 ABAST DEL PLA DIRECTOR DE SEGURETAT

L'abast del Pla Director de Seguretat a realitzar per l'Ajuntament de Riberola inclourà les infraestructures, xarxes i elements comentats en els punts anteriors, per tal de realitzar un estudi exhaustiu de la seguretat dels elements vinculats a les Tecnologies de la Informació i la Comunicació, així com els recursos humans relacionats amb aquests elements i que també són necessaris pel seu funcionament.

No es tractarà en cap cas la seguretat dels accessos físics de les diferents dependències amb l'excepció dels diferents Centres de Processament de Dades, així com tampoc es farà incís en la seguretat de la documentació física generada per l'organització. També s'exclou de l'àmbit la seguretat dels recursos humans de l'organització que no es vegin afectats ni estiguin relacionats amb cap dels actius analitzats durant el projecte actual, ja que determinats perfils de l'Ajuntament no interactuen en cap cas amb tecnologies de la informació i la comunicació (com poden ser brigades de jardineria, obra, pintura, etc.).

3. OBJECTIUS

Amb la implantació del **Pla Director de Seguretat** es pretén obtenir una visió de l'estat actual de la seguretat en els diferents elements relacionats amb les Tecnologies de la Informació i la Comunicació de l'Ajuntament de Riberola, proporcionar mesures o actuacions per millorar-ne els punts que puguin ser crítics per l'organització i assentar unes bases per a un **Sistema de Gestió de Seguretat de la Informació** per tal que el Pla Director de Seguretat vagi evolucionant al llarg del temps.

En cap cas es tracta d'eliminar totes les possibles vulnerabilitats o incidents, ja que això no és possible, i a més les inversions econòmiques queden limitades per la situació socioeconòmica en la que ens trobem actualment. Més aviat es tracta d'oferir un anàlisi de la situació actual i una fulla de ruta amb les diferents accions possibles a realitzar per tal de minimitzar riscos i impactes actuals.

Per tant, el Pla Director de Seguretat i el Sistema de Gestió de Seguretat de la Informació es poden convertir en unes eines imprescindibles per a que la direcció analitzi els riscos i possibles impactes periòdicament, escolleixi entre les diverses accions a realitzar segons la capacitat econòmica del moment i vagi evolucionant cap a uns sistemes més segurs.

Tot i així, el Pla Director de Seguretat requerirà l'execució i revisió de certs controls de manera periòdica per tal de revisar que les mesures existents i les que es vagin executant al llarg del temps estiguin funcionant correctament. Per tant, entrem en un cicle de PDCA (*Planificació-Fer-Comprovar-Actuar*), en que el Pla Director de Seguretat es va revisant, actualitzant i modificant segons vagin evolucionant els sistemes i processos de les Tecnologies de la Informació i Comunicació de l'organització.

Per tal d'assolir els objectius plantejats, al llarg del projecte es seguiran les normes de la família **ISO 27000**, és a dir, les **ISO/IEC 27001** i **ISO/IEC 27002**, publicades ambdues per la *International Organization for Standardization* (ISO) i la *International Electrotechnical Comission* (IEC). Aquestes normes recullen una sèrie de bones pràctiques (ISO 27002) i especificacions de requisits dels sistemes de gestió de seguretat de la informació (ISO 27001, norma certificable) per la gestió de la seguretat de la informació i estan àmpliament adoptades a milers d'empreses i organitzacions arreu del món.

Els objectius de l'organització al seguir el Pla Director de Seguretat principalment són:

- Millora de la seguretat de la informació de l'organització.
- Compliment de l'**Esquema Nacional de Seguretat**, LOPD 11/2007, etc.

- Coneixement en tot moment de l'estat actual de l'organització en matèria de seguretat.
- Informació respecte possibles millores a curt, mitjà i llarg plaç.
- Control periòdic de les mesures aplicades anteriorment.
- Estalvi de diners i/o temps en cas d'incident de seguretat.

4. ANÀLISIS DIFERENCIAL

La norma ISO/IEC 27001, en el seu Annex A, presenta 11 dominis, 39 objectius de seguretat i 133 controls a tenir en compte. Es divideix en diferents apartats que es poden resumir en:

- **APARTAT 1:** Abast
- **APARTAT 2:** Glossari
- **APARTAT 3:** Estructura de l'estàndard
- **APARTAT 4:** Anàlisi i gestió de riscos
- **APARTATS 5 AL 15:** Configuració dels diferents dominis amb els seus objectius de control de seguretat i els controls a implementar.

Els diferents dominis, número d'objectius i controls es poden observar en la *Figura 4-1,* extreta de [**UOC0**].

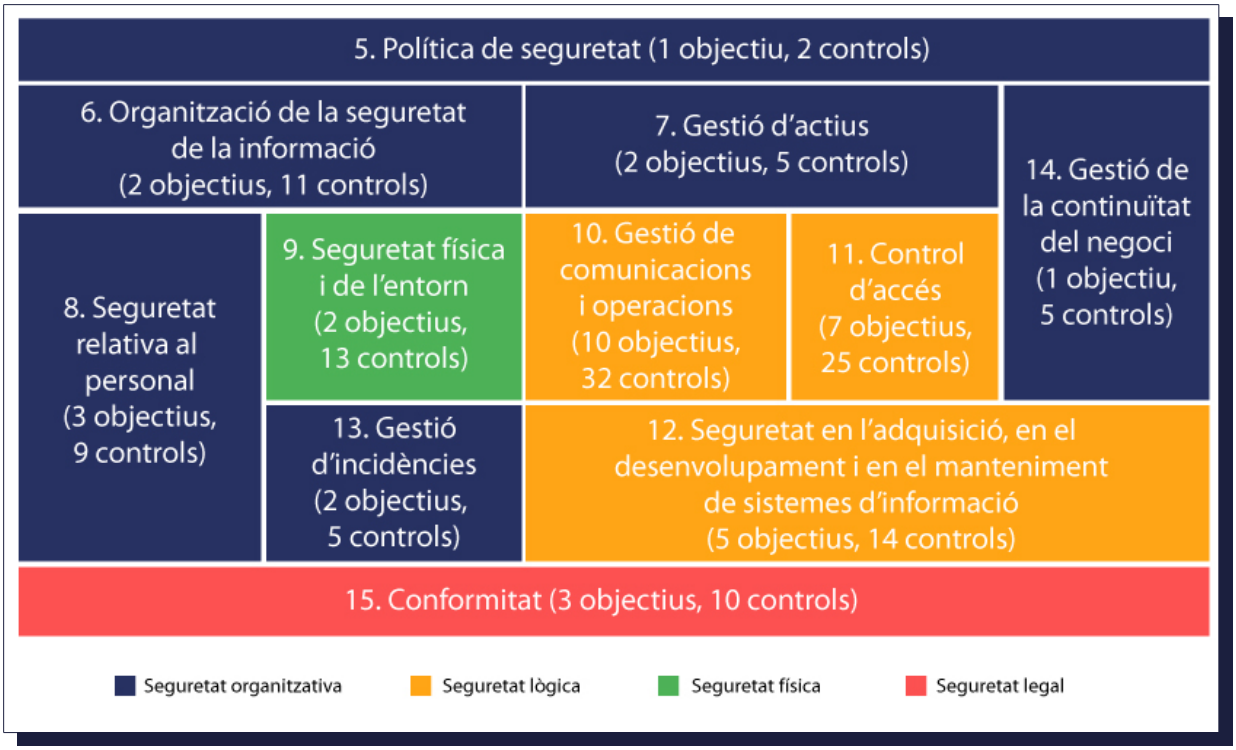

Figura 4-1: Dominis de la norma ISO/IEC 27002:2005

Seguir les bones pràctiques que s'esmenten en la ISO/IEC 27002 permetria a l'organització adaptar-se a l'Esquema Nacional de Seguretat relativa facilitat. L'Esquema Nacional de Seguretat no obliga a passar cap certificació respecte cap norma, però el Sistema Gestor de Seguretat de la Informació especificat en la ISO/IEC 27001 és aplicable.

4.1 ISO/IEC 27002 I ESQUEMA NACIONAL DE SEGURETAT

Moltes mesures de seguretat introduïts en l'ENS apareixen en la ISO/IEC 27002 [segons es pot consultar en **CCN0**]. Cal destacar però que l'Esquema Nacional de Seguretat és més específic i estableix un sistema de protecció proporcionat a la informació i els serveis a protegir, per racionalitzar la implantació de mesures de seguretat i reduir la discrecionalitat. D'altra banda, la norma ISO/IEC 27002 no disposa d'aquesta proporcionalitat i tot depèn de l'auditor que certifica la conformitat amb la ISO/IEC 27001.

Altres aspectes que els diferencien són que l'ENS fa esment d'aspectes relatius a la signatura electrònica, mentre que la norma ISO/IEC 27002 no en fa.

El següent quadre, extret de [**ISO1**] representa les **analogies i diferències** entre la norma ISO/IEC 27001 i l'Esquema Nacional de Seguretat (*Llistat 4-1*).

GESTIÓ SEGONS ISO 27001	GESTIÓ SEGONS L'ENS
El seu objectiu és la seguretat de la informació.	Regula els principis bàsics i estableix els requeriments mínims a tenir en compte.
Deixa llibertat per seleccionar l'abast del Sistema Gestor de Seguretat de la Informació.	Es refereix als mitjans electrònics utilitzats pels ciutadans en la seva relació amb les administracions públiques de l'estat.
S'enfoca als recursos en general, sense limitar-se als sistemes de la informació.	S'enfoca en el sistema d'informació (com a conjunt organitzat de recursos).
L'anàlisi de riscos s'ha de realitzar sempre.	L'anàlisi de riscos només és necessari per a sistemes de categoria mitja o alta (en matèria de seguretat).
No obliga a implementar mesures de seguretat concretes, tot i que si no s'apliquen es requereix una justificació.	Obliga a implantar un conjunt determinat de mesures de seguretat (segons la categoria del sistema tractat).
Exigeix la realització d'auditories periòdiques sobre l'abast del Sistema de Gestió de Seguretat de la Informació.	Exigeix una auditoria bianual de conformitat amb l'ENS per a sistemes de categoria mitja i alta (en matèria de seguretat).

Llistat 4-1: Analogies i diferències entre norma ISO/IEC 27001 i ENS.

Per tant, una gestió seguint les normes ISO/IEC 27001 ens aproxima molt al compliment de l'Esquema Nacional de Seguretat que persegueix l'organització.

4.2 ANÀLISI DIFERENCIAL

Per avaluar l'estat actual de l'organització davant de la ISO/IEC 27002, es presenta a continuació el *Llistat 4-2*, on es mostren cadascun dels controls dels diferents dominis associat a un valor segons els valors del model de maduresa CMMI que es mostren a la *Taula 4-2*. Amb aquesta informació s'obté una idea aproximada de com es troba l'aspecte de la seguretat en diferents àmbits de l'organització, ja que cadascun dels diferents nivells representa l'estat del procés dins l'organització:

Nivell	Descripció	Eficàcia	
L0	Inexistent	0%	No existeix cap tipus de procés ni acció referida al procés dins l'organització.
L1	Inicial / Ad hoc	10%	Els resultats de qualitat són deguts a les persones i a les eines emprades, però no als processos, els quals són inexistents.
L2	Reproduïble però intuïtiu	50%	Es duen a terme pràctiques bàsiques de gestió de projectes, de gestió de requisits, controls de versions i dels treballs fets per tercers.
L3	Procés definit	90%	Els processos estan prou documentats i accessibles als equips. El personal ha rebut formació.
L4	Mesurable i gestionat	95%	La qualitat del producte/pocés es mesura a partir de mètriques, que permeten establir l'evolució.
L5	Optimitzat	100%	Es disposa de mecanismes per a detectar punts de millora i introduir accions correctores, per a poder introduir el procés en un cicle de millora continua.

Taula 4-2: Diferents valors de maduresa del model CMMI.

Amb la taula de valoració anterior, ja estem capacitats per poder valorar cadascun dels

objectius que marca la ISO/IEC 27002.

5. POLÍTICA DE SEGURETAT	
5.1 Política de seguretat de la informació	
5.1.1 Document de política de seguretat *	L1
5.1.2 Revisió de la política de seguretat	L1
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ	
6.1 Organització interna	
6.1.1 Comitè de seguretat	L1
6.1.2 Coordinació	L2
6.1.3 Assignació de responsabilitats *	L3
6.1.4 Autorització de recursos	L5
6.1.5 Acords de confidencialitat	L5
6.1.6 Contacte amb autoritats	L5
6.1.7 Contacte amb altres grups d'interès	L4
6.1.8 Revisió independent	L1
6.2 Tercers	
6.2.1 Identificació de recursos	L3
6.2.2 Seguretat en la relació amb clients	L2
6.2.3 Seguretat en acords amb terceres parts	L3
7. GESTIÓ D'ACTIUS	
7.1 Responsabilitats sobre els actius	
7.1.1 Inventari d'actius	L2
7.1.2 Propietat dels actius	L4
7.1.3 Ús acceptable dels actius	L2
7.2 Classificació de la Informació	
7.2.1 Guies de classificació	L4
7.2.2 Marcatge i tractament de la informació	L2
8. SEGURETAT RELATIVA AL PERSONAL	
8.1 Abans de la contractació	
8.1.1 Rols i responsabilitats	L3
8.1.2 Selecció i política de personal	L5
8.1.3 Termes i condicions de la relació laboral	L2
8.2 Durant la relació laboral	
8.2.1 Supervisió d'obligacions	L3

8.2.2 Conscienciació, formació i capacitació en seguretat *	L2
8.2.3 Procediment disciplinari	L5
8.3 En finalitzar la contractació o canvi d'ocupació	
8.3.1 Cessació de responsabilitats	L5
8.3.2 Devolució d'actius	L5
8.3.3 Eliminació de drets d'accés	L5
9. SEGURETAT FÍSICA I DE L'ENTORN	
9.1 Àrees segures	
9.1.1 Perímetre de seguretat física	L3
9.1.2 Control d'accés físic	L5
9.1.3 Seguretat en oficines, despatxos i recursos	L4
9.1.4 Protecció enfront d'amenaces externes i d'entorn	L2
9.1.5 El treball en àrees segures	N/A
9.1.6 Accés públic, zones de càrrega i descàrrega	N/A
9.2 Seguretat en equips	
9.2.1 Ubicació i protecció	L4
9.2.2 Subministraments	L5
9.2.3 Seguretat del cablejat	L5
9.2.4 Manteniment dels equips	L3
9.2.5 Seguretat fora dels locals	L0
9.2.6 Reutilització o eliminació	L5
9.2.7 Autorització de sortida	L1
10. GESTIÓ DE COMUNICACIONS I OPERACIONS	
10.1 Procediments d'operació i responsabilitats	
10.1.1 Documentació de procediments	L0
10.1.2 Gestió de canvis	L1
10.1.3 Segregació de funcions	L4
10.1.4 Separació d'entorns desenvolupament i producció	L4
10.2 Gestió de la prestació de serveis per tercers	
10.2.1 Prestació de serveis	L4
10.2.2 Monitoratge i revisió de serveis	L4
10.2.3 Gestió de canvis en els serveis	L3
10.3 Planificació i acceptació del sistema	
10.3.1 Gestió de la capacitat	L5
10.3.2 Acceptació de sistemes	L5

10.4 Protecció conta codi maliciós	
10.4.1 Protecció contra codi maliciós	L3
10.4.2 Protecció contra codi descarregat en el client	L4
10.5 Gestió de suports i recuperació	
10.5.1 Recuperació de la informació	L5
10.6 Gestió de la seguretat de xarxes	
10.6.1 Controls de xarxa	L5
10.6.2 Seguretat dels serveis de xarxa	L5
10.7 Gestió de suports d'informació	
10.7.1 Gestió de suports extraïbles	L1
10.7.2 Retirada de suports	L4
10.7.3 Procediments d'utilització de la informació	L1
10.7.4 Seguretat en la documentació dels sistemes	L5
10.8 Intercanvi d'informació	
10.8.1 Polítiques i procediments d'intercanvi d'informació	L1
10.8.2 Acords d'intercanvi	L4
10.8.3 Suports físics en trànsit	L1
10.8.4 Missatgeria electrònica	L4
10.8.5 Sistemes d'informació del negoci	L4
10.9 Serveis de comerç electrònic	
10.9.1 Comerç electrònic	N/A
10.9.2 Transaccions en línia	N/A
10.9.3 Informació d'accés públic	L5
10.10 Monitoratge	
10.10.1 Registre d'activitats	L3
10.10.2 Ús dels sistemes de monitoratge	L5
10.10.3 Protecció de les traces i registres	L3
10.10.4 Traces d'administració i operació	L3
10.10.5 Registre de fallades	L2
10.10.6 Sincronització de rellotges	L3
11. CONTROL D'ACCÉS	
11.1 Requisits de negoci pel control d'accés	
11.1.1 Política de control d'accés	L2
11.2 Gestió d'accés dels usuaris	
11.2.1 Registre d'usuaris	L2

11.2.2 Gestió de privilegis	L4
11.2.3 Gestió de contrasenyes d'usuari	L3
11.2.4 Revisió dels drets d'accés d'usuari	L1
11.3 Responsabilitat dels usuaris	
11.3.1 Ús de credencials	L2
11.3.2 Equips d'usuaris desatesos	L3
11.3.3 Política de taules i pantalles netes	L1
11.4 Control d'accés a la xarxa	
11.4.1 Política d'ús dels serveis de la xarxa	L4
11.4.2 Autenticació d'usuaris per a connexions remotes	L5
11.4.3 Autenticació de nodes a la xarxa	L5
11.4.4 Protecció dels ports de diagnòstic i configuració remots	L4
11.4.5 Segregació de les xarxes	L5
11.4.6 Control de la connexió a la xarxa	L3
11.4.7 Control d'encaminament a la xarxa	L4
11.5 Control d'accés al sistema operatiu	
11.5.1 Procediments de connexió	L5
11.5.2 Identificació i autenticació d'usuaris	L5
11.5.3 Sistema de gestió de contrasenyes	L1
11.5.4 Ús dels serveis del sistema	L3
11.5.5 Desconnexió automàtica de sessió	L1
11.5.6 Limitació del temps de connexió	L3
11.6 Control d'accés a la informació i a les aplicacions	
11.6.1 Restricció d'accés a la informació	L5
11.6.2 Aïllament de sistemes sensibles	L4
11.7 Informàtica mòbil i teletreball	
11.7.1 Informàtica mòbil i comunicacions	L2
11.7.2 Teletreball	N/A
12. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE SISTEMES D'INFORMACIÓ	
12.1 Requisits de seguretat en sistemes d'informació	
12.1.1 Anàlisi i especificació de requisits	L3
12.2 Control de processos en aplicacions	
12.2.1 Validació de dades d'entrada	L4
12.2.2 Control de processos interns	L1
12.2.3 Integritat de missatges	L5
12.2.4 Validació de dades de sortida	L4

12.3 Controls criptogràfics	
12.3.1 Política d'ús de controls criptogràfics	L3
12.3.2 Xifratge	L4
12.4 Seguretat dels fitxers de sistema	
12.4.1 Control de programari en producció	L5
12.4.2 Protecció de dades de prova	L4
12.4.3 Control d'accés al codi font	L3
12.5 Seguretat en el desenvolupament i en el suport	
12.5.1 Procediments de control de canvis	L1
12.5.2 Revisió tècnica de canvis en el sistema operatiu	L5
12.5.3 Restricció de canvis en paquets de programari	L3
12.5.4 Fuites d'informació a través del codi	L4
12.5.5 Externalització de desenvolupament de programari	L4
12.6 Gestió de les vulnerabilitats tècniques	
12.6.1 Control de les vulnerabilitats tècniques	L3
13. GESTIÓ D'INCIDÈNCIES DE SEGURETAT DE LA INFORMACIÓ	
13.1 Notificació d'incidències i debilitats *	
13.1.1 Notificació d'esdeveniments de seguretat	L3
13.1.2 Notificació de debilitats	L3
13.2 Gestió d'incidències i millora *	
13.2.1 Identificació de responsabilitats i procediments	L2
13.2.2 Avaluació d'incidències	L1
13.2.3 Recol·lecció d'evidències	L1
14. GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI *	
14.1 Gestió de la continuïtat del negoci	
14.1.1 Procés de gestió de la continuïtat del negoci	L2
14.1.2 Continuïtat de negoci i anàlisi d'impacte	L2
14.1.3 Documentació i implantació del pla de continuïtat	L1
14.1.4 Marc de planificació	L2
14.1.5 Procés, manteniment i avaluació de Plans de continuïtat	L2
15. CONFORMITAT	
15.1 Conformitat amb requisits legals	
15.1.1 Identificació de la legislació aplicable	L5
15.1.2 Dret de la propietat intel·lectual *	L5
15.1.3 Control de seguretat de registres de l'organització *	L3

15.1.4 Protecció dades de caràcter personal i de la intimitat *	L5
15.1.5 Evitar mal ús de recursos de tractament de la informació	L3
15.1.6 Reglamentació de controls de xifratge	L4
15.2 Compliment del marc normatiu	
15.2.1 Compliment de polítiques i normes	L0
15.2.2 Comprovació de la conformitat tècnica	L0
15.3 Auditoria de sistemes	
15.3.1 Controls d'auditoria de sistemes	L0
15.3.2 Protecció d'eines d'auditoria	L0

Llista 4-2: Compliment dels diferents controls - Estat actual

En el *Llistat 4-2* es poden observar els elements o controls que cal implementar obligatòriament per tal de complir amb la norma (controls marcats amb el caràcter ' * ').

Amb els valors quantitatius (%) per cadascun dels nivells representats en un gràfic de tipus radar, podrem observar àgilment i de manera gràfica en quin punt de compliment de l'estàndard es troba l'organització per cadascun dels diferents dominis (*Figura 4-2*):

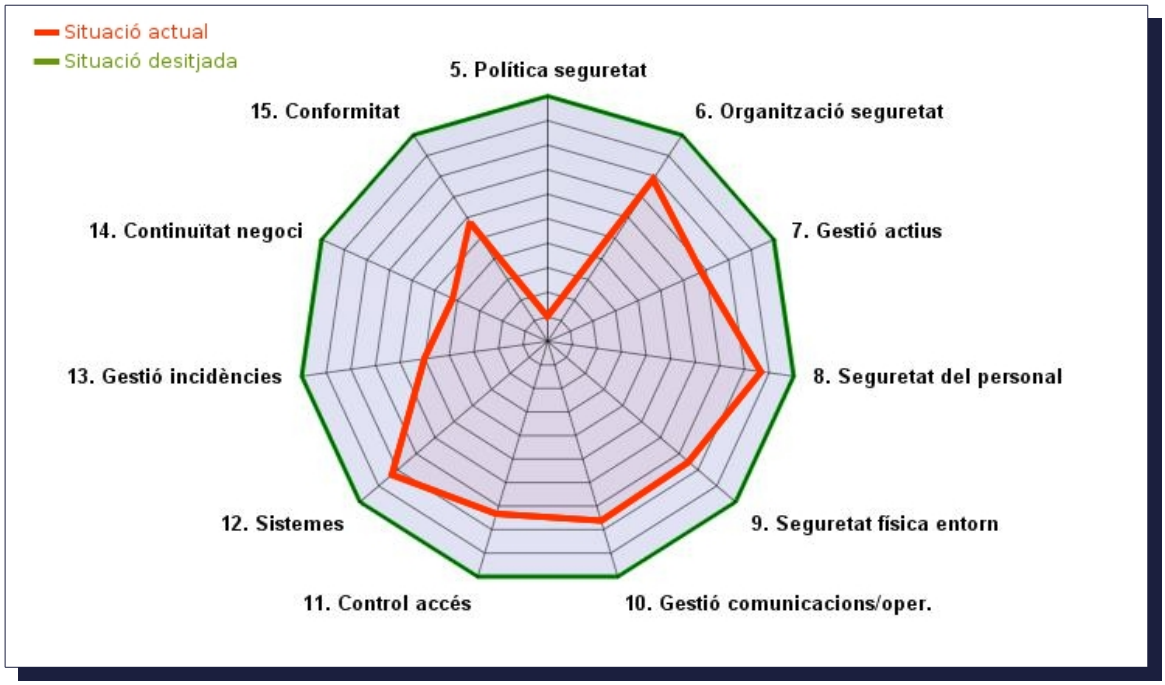

Figura 4-2: Gràfic tipus radar amb valoració actual de l'organització

5. SISTEMA DE GESTIÓ DOCUMENTAL

5.1 POLÍTICA DE SEGURETAT

La **política de seguretat** de la informació estableix unes bases i línies d'actuació globals per, alineats amb els objectius del negoci (tal i com es pot llegir en [**UOC0**]).

La política cal que demostri el **compromís de la direcció** amb la seguretat de la informació, i cal que se n'informi als usuaris dels diferents sistemes que formen part de les infraestructures de l'organització.

Una definició estàndard i formal la podem trobar en el punt 3.1 del RFC 1244 (*Request for Comments - Site Security Handbook* del IETF, consultable en [**RFC0**]), on es cita:

> *"La política de seguretat defineix el què necessita ser protegit, el que és més important, quines prioritats hi ha en l'organització i quina és l'aproximació general que hi hauria d'haver per els problemes de seguretats potencials.*
>
> *La política de seguretat pe si mateixa no diu com estan protegits els elements. Aquest és el rol dels procediments de seguretat."*

Per tant, una política de seguretat cal que estableixi les necessitats i requisits de protecció, a molt alt nivell, dins l'àmbit de l'organització. Així mateix, aquesta política pot estar acompanyada d'altres documents de rang inferior per tal de concretar i aprofundir més en els principis i objectius de seguretat establerts. Aquests documents poden ser, tal i com es pot consultar en [**INT0**]:

- **Normes de seguretat**
- **Procediments de seguretat**
- **Procediments operatius de seguretat**
- **Instruccions tècniques**

La **política de seguretat** definida per l'Ajuntament de Riberola, basada en bona part en la Política de Seguretat creada per l'Ajuntament de Màlaga [**POL0**], es pot consultar en l'**Apartat A.1** de l'**Annex I** del present document. La Política que es presenta ha estat redactada i està actualment en procés de revisió, però no ha estat aprovada per la Junta de Govern Local de l'Ajuntament, per tant encara no s'aplica.

5.2 PROCEDIMENT D'AUDITORIES INTERNES

Anualment es realitzarà una auditoria interna per comprovar si els controls, processos i procediments del Sistema de Gestió de Seguretat de la Informació segueix conforme la norma i la legislació vigent, així com validar que els objectius de seguretat de l'organització estan implementats, mantinguts amb eficàcia i tenen el rendiment esperat.

Les característiques principals de l'auditoria interna són:

1. **L'auditoria ha de ser independent:** no es pot considerar adequada una auditoria realitzada pel propi personal que han implantat o que gestiona el sistema.
2. **Experiència de l'auditor:** Per obtenir unes recomanacions adequades cal que l'auditor disposi d'experiència suficient en el sector.
3. **Estructura del document:** Haurà d'incloure, com a mínim:
    - Declaració d'abast i objectius.
    - Opinió i conclusions respecte funcionament de controls i procediments.
    - Problemes o incidències detectades.
    - Excepcions.
    - Accions correctives a portar a terme.
    - Accions complementàries en cas que siguin necessàries.
    - Recomanacions.
    - Limitacions.
    - Declaració respecte les directrius seguides.

El resultat de cada auditoria quedarà degudament registrat dins el Sistema Gestor de Seguretat de la Informació. El Comitè de Seguretat haurà d'estudiar possibles projectes seguint les recomanacions sorgides de l'auditoria interna, per tal de presentar-los a la Junta de Govern Local.

El document amb el Procediment d'auditories internes es pot consultar en l'**Apartat A.2** de l'**Annex I**, i es basa en un document model que es pot trobar en *ISO 27001 Toolkit* [**ISO4**].

5.3 GESTIÓ D'INDICADORS

Els indicadors permeten controlar el funcionament de les diferents mesures de seguretat de la informació implantades, així com també l'eficàcia i eficiència que tenen. Cal definir-ne els mecanismes i la periodicitat de mesura de cadascun dels indicadors.

És imprescindible implantar indicadors per poder conèixer l'eficiència de cadascun dels controls. Per tant, cada control ha de disposar d'almenys un indicador, tot i que els indicadors poden fer referència a més d'un control.

Tot indicador consta de vuit components bàsics (segons es pot veure en [**UOC0**]):

1. **Nom de l'indicador:** cal que sigui significatiu però no massa llarg.
2. **Descripció:** explicació de l'objectiu de mesura de l'indicador.
3. **Control(s) de seguretat relacionat(s):** llista on s'indica quin control o controls cobreix l'indicador.
4. **Fórmula de mesurament:** cal que la fórmula estigui calculada mitjançant paràmetres concrets que no es prestin a ambigüitat.
5. **Unitats de mesura:** cal especificar les unitats de mesura.
6. **Freqüència de mesura:** indica amb quina periodicitat cal recollir la mesura.
7. **Valor objectiu i valor llindar:** quan sigui possible, cal assignar quin és el valor que l'organització assumeix com a correcte i sota per quin valor cal generar una alerta.
8. **Responsable de la mesura:** indica a quin càrrec recau la responsabilitat de proporcionar el resultat de la mesura.

Se'n pot consultar la plantilla per la fitxa d'un indicador en l'**Annex I**, **Apartat A.3**.

Es poden consultar els indicadors existents pels diferents objectius de control en l'**Annex I**, **Apartat A.4**.

5.3.1 TIPUS D'INDICADORS

En [**UOC0**] i [**ISO5**] disposem d'exemples d'indicadors per poder tenir una idea de quina mesura implementar segons la tipologia del control a analitzar:

- **Indicadors de gestió:**
  - Nombre d'hores de formació impartides al personal de l'organització.
  - Pressupost de l'entitat destinat a personal de manteniment de sistemes.
  - Número de treballadors amb responsabilitats en processos vinculats a la seguretat de la informació.
  - Nombre de suggeriments de millora rebuts per part de treballadors i/o direcció.
  - Enquestes a mostra significativa de plantilla de treballadors o departament

involucrat en el control, mitja ponderada de les respostes correctes respecte el total.

- **Indicadors d'operació:**
  - Temps total de caiguda o disponibilitat d'un servei durant un període de temps determinat.
  - Nombre d'avaries d'un tipus d'equipament informàtic o de telecomunicacions.
  - Trànsit mitjà del tallafoc.
  - Ocupació de memòria i disc respecte el total disponible dels servidors.
  - Detecció de certes tipologies de tràfic en l'IDS (per exemple P2P).
  - Nombre de virus detectats respecte incidències o avaries provocades per aquests codis maliciosos.
- **Indicadors d'entorn:**
  - Alertes per nous virus i codis maliciosos.
  - Temps mitjà d'exposició d'un sistema des de detecció de vulnerabilitat fins aplicació de la correcció.
  - Alertes per inclemències del temps.
  - Canvis en la legislació vigent.

5.3.2 PAUTES D'IMPLANTACIÓ

Per la implantació d'indicadors cal seguir les següents pautes (segons [**UOC0**]):

- Cada control ha de ser analitzat com a mínim per un indicador.
- Un mateix indicador es pot aplicar a diversos controls, un objectiu o fins i tot a seccions completes de la norma.
- Inicialment serveixen per controlar la implantació, posteriorment afecten al procés de millora continua.
- No s'han d'implantar indicadors no rellevants donat que impliquen una destinació de recursos de l'organització.
- Cal ser rigorós en la recollida de la informació, ja que aquestes dades han de ser fiables, representatives i comparables en un futur.
- La informació que aporten ha de ser de rellevància.

- Caldrà comparar els seus valors en el temps, per tant cal mantenir-ne la seva escala de valors. Molta cura en la reflexió inicial de controls.
- En la mesura que sigui possible, cal automatitzar la mesura dels indicadors.
- L'esforç per obtenir el mesurament ha de ser proporcional al valor de la informació que proporciona.

5.4 PROCEDIMENT DE REVISIÓ PER DIRECCIÓ

Per tal de poder realitzar una revisió periòdica per part de direcció, es crea un procediment de revisió per direcció de l'estat actual del SGSI. Aquest procediment es pot consultar en l'**Apartat A.5** de l'**Annex I**.

Aquesta revisió del Sistema Gestor de Seguretat de la Informació és obligada com a mínim un cop l'any, i té com a objectiu assegurar que és adequat i efectiu pels propòsits i context de l'organització.

5.5 GESTIÓ DE ROLS I RESPONSABILITATS

L'òrgan de direcció de l'Ajuntament de Riberola és, com a qualsevol administració local de nuclis de més de 5.000 habitants, la Junta de Govern Local. Es tracta d'un òrgan col·legiat necessari pel govern municipal que, solta la presidència de l'alcalde, està integrat per un nombre de regidors no superior al terç del nombre legal dels membres corporatius, nomenats i separats lliurement per aquell, donant-ne compte, posteriorment, al Ple.

L'alcalde determinarà, mitjançant decret, el nombre de membres de la Junta de Govern Local, així com els regidors que hagin de posseir tal condició. La condició de membre de la Junta de Govern Local és de caràcter voluntari.

A la Junta de Govern Local, com a òrgan executiu, li corresponent les següents competències:

1. L'assistència a l'alcalde en l'exercici de les seves atribucions.
2. Les atribucions que el Ple li delegui.
3. Les atribucions que l'alcalde li delegui.
4. Les atribucions que, directament, li atribueixin les lleis estatals o autonòmiques.

D'altra banda, el consistori disposa d'una Regidoria de Tecnologies de la Informació i Comunicació. Per tal de tenir un membre comú en la Junta de Govern Local i en el Comitè de Seguretat, s'ha decidit que el Regidor de Tecnologies de la Informació i Comunicació també formi part del Comitè de Seguretat. Això implicarà una millora en la coordinació dels dos

òrgans.

La documentació formal dels diferents rols i responsabilitats definits per l'Ajuntament de Riberola es pot consultar en l'**apartat A.6** de l'**Annex I**.

5.6 METODOLOGIA D'ANÀLISI DE RISCOS

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

El Consell Superior d'Administració Electrònica (CSAE) de l'Estat espanyol elabora i promou MAGERIT com a resposta a la percepció de que l'Administració Pública, i en general tota la societat, depenen cada vegada de manera més significativa dels sistemes d'informació a l'hora d'assolir els seus objectius. L'ús de les tecnologies de la informació i la comunicació suposen molts beneficis per les administracions, empreses i ciutadans, però al mateix temps impliquen certs riscos que cal gestionar mitjançant mesures de seguretat.

Per tant, Magerit ens aporta una metodologia per poder analitzar i gestionar els diferents riscos existents en qualsevol tipus d'organitzacions, ja siguin administracions públiques o empreses.

5.6.1 ANTECEDENTS

El Real Decret 3/2010, del 8 de gener, amb el qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, esmenta en el Capítol 2, Principis Bàsics:

> *Article 6. Gestió de la seguretat basada en els riscos.*
>
> *1. L'anàlisi i gestió de riscos serà part essencial del procés de seguretat i haurà de mantenir-se permanentment actualitzat.*
>
> *2. La gestió de riscos permetrà el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitzarà mitjançant el desplegament de mesures de seguretat que estabiliran un equilibri entre la naturalesa de les dades i els tractaments, els riscos als que estan exposades i les mesures de control.*

El mateix Real Decret 3/2010, en el Capítol III, Requisits mínims, s'esmenta:

> *Article 13. Anàlisi i gestió dels riscos.*

> *1. Cada organització que desenvolupi o implanti sistemes pel tractament de la informació i les comunicacions realitzarà la seva pròpia gestió de riscos.*
>
> *2. Aquesta gestió es realitzarà mitjançant de l'anàlisi i el tractament dels riscos als que està exposat el sistema. Sense perjudici de lo exposat en l'Annex II, s'emprarà alguna metodologia reconeguda internacionalment.*
>
> *3. Les mesures adoptades per tal de reduir o suprimir els riscos hauran de ser justificades, i en tot cas, existirà una proporcionalitat entre aquestes mesures i els riscos.*

La Llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics, en el seu Article 1, Objectiu de la Llei diu així:

> *2. Les Administracions Públiques utilitzaran las tecnologies de la informació d'acord amb lo disposat en la present Llei, assegurant la disponibilitat, l'accés, la integritat, l'autenticitat, la confidencialitat i la conservació de les dades, informacions i serveis que gestionen en l'exercici de les seves competències.*

Finalment, la Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal, en el seu article 9 (Seguretat de les dades) diu així:

> *1. El responsable del fitxer, i, en el seu cas, l'encarregat del tractament, hauran d'adoptar les mesures tècniques i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia existent, la naturalesa de les dades emmagatzemades i els riscos als que estan exposades, ja siguin originats per acció humana, medi físic o natural.*

Per tal d'adaptar-se a la legislació vigent segons el Real Decret 3/2010, l'Ajuntament de Riberola seguirà la metodologia Magerit versió 3 per tal de realitzar l'anàlisi i gestió dels riscos relacionats amb les tecnologies de la informació i la comunicació.

5.6.2 OBJECTIUS A MAGERIT

Magerit és una metodologia d'anàlisi i gestió de riscos que persegueix els següents

objectius (extrets de [MAG0]):

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

5.6.3 VISIÓ DE CONJUNT

El procés de **gestió de riscos** està format principalment per dos tasques:

1. **Anàlisi de riscos:** permet determinar què té l'Organització i preveure el que podria succeir.
2. **Tractament dels riscos:** permet organitzar les mesures per evitar possibles problemes i al mateix temps estar preparats per tractar emergències, sobreviure a incidents i seguir operant amb les millors condicions, assumint un risc residual que sempre existirà.

L'anàlisi de riscos mitjançant Magerit considera els següents elements:

- **actius:** són els elements del sistema de la informació (o molt lligats a aquests elements) que suporten les activitats i processos de l'organització. Pot existir una relació de dependència jeràrquica entre ells (per exemple "*CPD -> Servidor -> Servei de correu*").
- **amenaces:** són esdeveniments o fets que poden succeir als actius, provocant un perjudici concret a l'organització.
- **contramesures:** són mesures de protecció desplegades per a reduir possibles danys provocats per les diferents amenaces existents.

Amb els elements definits anteriorment podem determinar ara els següents conceptes que també proporciona Magerit:

- **impacte:** defineix l'efecte per l'organització si una amenaça es convertís en realitat.
- **risc:** probabilitat que succeeixi l'amenaça.

L'anàlisi de riscos mitjançant la metodologia Magerit permet analitzar els elements definits anteriorment de forma metòdica en tota l'organització, per tal d'extreure unes conclusions i procedir al tractament dels riscos que en sorgeixin. En la *Figura 5.1* es pot observar la relació sobre els diferents conceptes comentats:

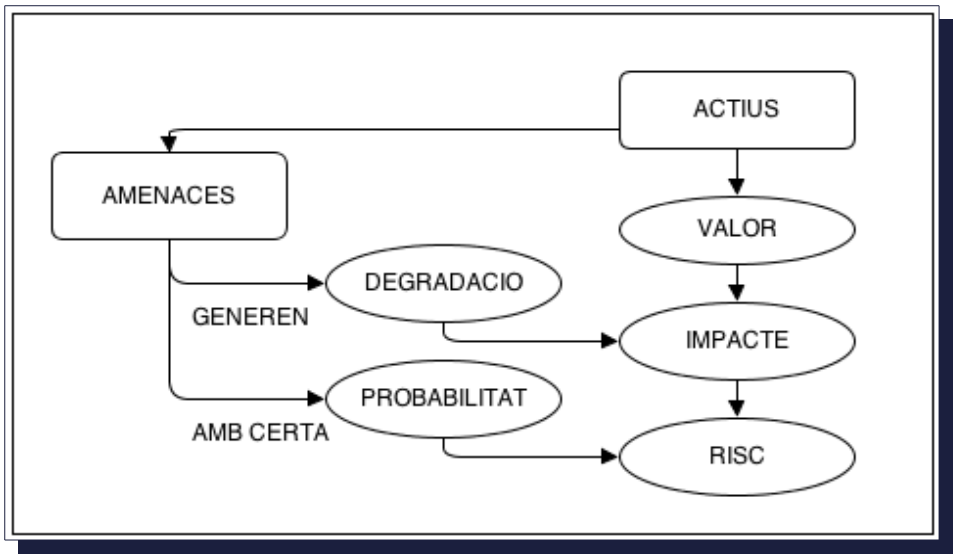

Figura 5.1: Relació dels elements que intervenen en la gestió de riscos.

Tal i com es pot observar en la Figura 5.1, l'organització disposa d'uns actius degudament identificats. Aquests actius tenen un valor per l'organització, i una incidència sobre aquests actius pot provocar un determinat impacte en alguna de les dimensions dels actius (confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat).

Per aquests actius existeixen unes amenaces que poden succeir per degradació dels actius o de forma espontània, tot i que l'amenaça pugui ser poc probable. Contra aquest tipus d'amenaces cal proporcionar les contramesures apropiades per tal de reduir el risc pels actius.

5.6.4 FASES DE MAGERIT

La metodologia consisteix en l'execució de les següents fases (segons[**UOC0**]):

1. Presa de dades. Processos de la informació.
2. Dimensionament. Establiment de paràmetres.
3. Anàlisi d'actius.
4. Anàlisi d'amenaces.
5. Establiment de vulnerabilitats.
6. Establiment d'impactes.

7. Anàlisi de risc intrínsec.
8. Influència de controls de seguretat.
9. Anàlisi de riscos efectius.
10. Avaluació de riscos.

5.6.5 ESTABLIMENT DE PARÀMETRES – VALORACIÓ D'ACTIUS

Una part molt important de la metodologia consisteix en la realització de les valoracions i l'assignació d'uns determinats valors segons aquestes valoracions. Per tant, cal assignar als diferents actius de l'organització un valor que en determini la seva importància.

Aquesta assignació de valors no és senzilla, ja que cal considerar, si s'escauen, el valor de reposició de l'actiu, el de configuració, el seu valor d'ús per part de l'organització i el de pèrdua d'oportunitat per no disposar de l'actiu. Per tant, potser un actiu no val econòmicament 300.000 €, però la importància d'aquest actiu és vital per l'organització i per tant se li assigna una valoració com a actiu de "Molt alta". Aquest punt cal tenir-lo molt en compte ja que al tractar-se d'una administració pública, encara és més complicat donar un valor econòmic a certs actius (sobretot si es tracta de dades). Per tant, de cara la valoració dels actius podem optar per fer-ho de manera qualitativa, tot i que de cara a Magerit també disposarem d'una suposada valoració econòmica (i per tant quantitativa).

Per tal de realitzar aquesta tasca utilitzarem la següent taula de valoracions (*Taula 5.1*):

Valoració	Rang	Valor
Molt alta	Valor > 200.000 €	300.000 €
Alta	Valor entre 100.000 € i 200.000 €	150.000 €
Mitjana	Valor entre 50.000 € i 100.000 €	75.000 €
Baixa	Valor entre 10.000 € i 50.000 €	30.000 €
Molt baixa	Valor < 10.000 €	10.000 €

Taula 5.1: Valoració d'actius

Cal tenir en compte que els actius estan o poden estar relacionats de manera jeràrquica. Per exemple, el servei de correu electrònic (actiu) està relacionat amb un servidor (actiu) que es troba dins un CPD (actiu). Per tant, el servei de correu electrònic estarà afectat no només pels riscos inherents a un servei de correu electrònic, sinó als riscos dels actius dels

quals depèn.

5.6.6 ESTABLIMENT DE PARÀMETRES – DIMENSIONS DE SEGURETAT

Un cop identificats els actius i feta la seva valoració, en caldrà calcular la seva criticitat. Aquesta operació caldrà realitzar-la per cadascuna de les diferents dimensions de seguretat que estableix Magerit (Llibre I – Mètode, pàgina 24 [**MAG0**]), sempre i quan tinguin sentit per l'actiu. Aquestes dimensions que cal considerar són:

- Disponibilitat
- Integritat
- Traçabilitat
- Confidencialitat
- Autenticitat

5.6.7 ESTABLIMENT DE PARÀMETRES – VALORACIÓ DE VULNERABILITATS

En Magerit, les vulnerabilitats representen la freqüència d'ocurrència d'una amenaça. Aquesta freqüència també cal plasmar-la en una escala de valors que es pot consultar en la *Taula 5.2:*

Vulnerabilitat	Rang	Valor
Freq. extrema	1 vegada al dia	1
Freq. alta	1 vegada cada 2 setmanes	0,071233
Freq. mitjana	1 vegada cada 2 mesos	0,016438
Freq. baixa	1 vegada cada 6 mesos	0,005479
Freq. molt baixa	1 cop l'any	0,002739

Taula 5.2: Valoració de vulnerabilitats

En la taula anterior, el valor estadístic que es mostra coincideix amb la **freqüència estimada d'una amenaça / dies de l'any**, considerant que any té 52 setmanes.

5.6.8 ESTABLIMENT DE PARÀMETRES – VALORACIÓ DELS IMPACTES

Entenent per impacte el tant per cent del valor de l'actiu que es perd en cas d'incidència, es farà referència a la *Taula 5.3* de valoració d'impactes.

Vulnerabilitat	Valor
Molt alt	100%
Alt	75%
Mitjà	50%
Baix	20%
Molt baix	5%

Taula 5.2: Valoració d'impactes

Caldrà calcular l'impacte per cadascuna de les diferents dimensions de l'actiu, tenint en compte els actius dels que depèn.

5.6.9 ESTABLIMENT DE PARÀMETRES – VALORACIÓ DELS CONTROLS DE SEGURETAT

Amb els valors comentats en els apartats anteriors es podrien calcular els impactes i els riscos als que estan exposats els actius, sempre i quan no tinguessin cap control o protecció. Cal doncs considerar ara la valoració dels controls de seguretat existents dels diferents actius. La valoració de les contramesures existents en l'organització s'extraurà de la següent taula (*Taula 5.3*):

Efectivitat	Valor
Molt alta	95%
Alta	75%
Mitjana	50%
Baixa	30%
Molt baixa	10%

Taula 5.2: Valoració de controls existents

Tal i com es pot observar a la Taula 5.2, mai un control rebrà una efectivitat del 100%. Les efectivitats dels diferents controls poden ser diferents per les diferents dimensions de seguretat comentades en l'apartat 5.6.6.

5.6.10 AMENACES

Magerit, en el seu Llibre II, apartat 5 [**MAG1**], ofereix una llista de possibles amenaces, juntament amb el tipus d'actius i dimensions afectades, així com una breu descripció, dividides en cinc tipologies principals:

- [N] – Desastres naturals
- [I] – D'origen industrial
- [E] – Errors no intencionats
- [A] – Atacs intencionats

5.7 DECLARACIÓ D'APLICABILITAT

La declaració d'aplicabilitat consisteix en un document principal on es defineix com s'implementarà gran part del sistema de seguretat de la informació. El seu objectiu principal és, tal i com es pot llegir en **[DDA0]**, l'especificació de quins dels 133 controls disponibles (mesures de seguretat) són els que implementarà l'organització, especificant les raons contemplar-los o no, i dels seleccionats resumint com s'ha realitzat el control.

És el document de referència que es seguirà en una auditoria de certificació, on es comprovarà que cadascun dels controls s'han implementat tal i com s'informa a la declaració d'aplicabilitat. La declaració d'aplicabilitat de l'Ajuntament de Riberola es pot consultar en l'**Annex I**, **apartat A.7**.

6. ANÀLISI DE RISCOS

En l'anàlisi de riscos cal tenir molt en compte els processos crítics de l'organització, ja que determinaran quins actius afecten aquests processos. La possible afectació o cost econòmic dels actius proporcionarà un valor més o menys estimatiu d'aquest element per l'organització.

D'altra banda, cadascun d'aquests actius es pot veure afectat per una o més amenaces amb una certa probabilitat, que pot ser diferent per cadascuna de les diferents dimensions de seguretat (**A**utenticitat, **C**onfidencialitat, **I**ntegritat, **D**isponibilitat i **T**raçabilitat).

Finalment, amb les amenaces determinades per cadascun dels actius podrem establir un impacte per l'organització en cas que una amenaça es materialitzi. Aquestes dades permeten a l'organització establir prioritats, tractant d'aplicar contramesures a les amenaces que presentin un major impacte per l'organització. D'aquesta manera, un possible impacte es veurà reduït si per l'actiu corresponent s'hi apliquen contramesures i controls.

Cal considerar que tot i reduir els possibles impactes, sempre existeix un risc anomenat residual. Aquest risc ha d'estar acceptat per la direcció de l'organització i cal definir quin és el nivell d'impacte mínim que es considera residual.

6.1 INVENTARI D'ACTIUS

Per tal de poder dividir els actius, Magerit proposa classificar-los en les següents categories [consultable en **MAG1**, *Apartat 2 - Tipus d'actius*]:

- **[D] - Dades:** Contenen la informació que permet a una organització prestar els seus serveis. És un actiu abstracte que pot ser transmès o emmagatzemat en equips o suports d'informació. Exemples: fitxers, bases de dades, còpies de seguretat, dades de configuració, contrasenyes, registres d'activitat, etc.
- **[K] - Claus criptogràfiques:** S'empren per protegir el secret o autenticar les diferents parts d'una comunicació. Les claus són essencials per garantir el funcionament dels mecanismes criptogràfics. Exemple: claus privades de tokens o targetes criptogràfiques.
- **[S] - Serveis:** Funció que satisfà una necessitat als usuaris (del servei). Poden ser anònims (sense requerir autenticació d'usuari), al públic en general, a usuaris externs (amb relació contractual) o a usuaris interns, els quals formen part de l'organització.

Exemple: consulta de padró (usuaris interns), tràmits en línia (públic general, però amb autenticació) o pàgina web (servei anònim).

- **[SW] - Software/aplicacions informàtiques:** Les aplicacions d'una organització gestionen, analitzen i transformen les dades permetent l'explotació d'aquesta informació per la prestació de serveis. És important destacar que el codi font d'aplicacions pròpies desenvolupades per la mateixa organització constaria com a dades, mentre que el programa resultant si seria considerat aplicació. Exemples: Sistemes operatius, antivirus, aplicacions d'ofimàtica, servidor de correu, client de correu, etc.
- **[HW] - Maquinari/hardware:** Mitjans materials físics destinats a suportar, directa o indirectament els serveis que presta l'organització, essent dipositaris temporals o permanents de les dades. Exemple: Servidor, estació de treball, portàtil, PDA, electrònica de xarxa, etc.
- **[COM] - Xarxes de comunicacions:** Mitjans de transport que transporten dades d'un lloc a un altre. Exemples: Internet, routers, xarxes sense fil WiFi, telefonia mòbil, etc.
- **[Media] - Suports d'informació:** Dispositius físics que permeten emmagatzemar informació de forma permanent o durant llargs períodes de temps. A diferència del maquinari, aquests suports no són capaços de tractar la informació, només d'emmagatzemar-la. Exemples: memòries USB, disc durs, DVD, cintes magnètiques, etc.
- **[AUX] - Equipament auxiliar:** en aquest punt Magerit es refereix als elements de suport als sistemes de la informació, sense estar relacionats directament amb el tractament de dades. Per exemple: sistemes de refrigeració, sistemes d'alimentació ininterrompuda, cablejat, robots de cinta, caixes fortes, equips de destrucció, etc.
- **[L] - Instal·lacions:** llocs on s'allotgen els sistemes de la informació. Poden ser plataformes mòbils com cotxes o camions, tot i que generalment es tractarà de Centres de Processament de Dades i edificis on l'organització desenvolupa les seves activitats.
- **[P] – Personal:** en aquest punt s'hi classificaran les persones vinculades als sistemes de la informació.

Magerit proporciona més classificacions i divisions dels possibles actius, però degut a l'abast del projecte actual no es desitja entrar més en detall. Tot i així, es important destacar que es podria ser més específics amb l'inventari d'actius en cas que l'abast de l'anàlisi de riscos ho

requerís, però cal tenir present que un anàlisi més detallat implica un cost addicional que caldria ser assumit per part de la direcció.

A l'hora de realitzar l'inventari cal tenir en compte, a més dels processos crítics en els quals intervenen els actius, la jerarquia que existeix entre ells. Per exemple, si un servidor allotja una base de dades imprescindible, l'actiu de la base de dades (actiu superior) es veurà afectat per les possibles amenaces que afecten al servidor (actiu inferior). Per tant, cal elaborar aquest arbre de dependències dels actius per obtenir una correcta valoració dels riscos. En general, segons es pot veure en el llibre de la metodologia Magerit **[MAG0]**, les dependències dels actius generalment venen donades per un esquema de dependències entre capes, tot i que cal adaptar-se a les necessitats específiques per cada projecte.

Per tant, cada capa superior dependrà, en general, d'elements de la mateixa capa o de capes inferiors. L'esquema es mostra en la Figura 6-1.

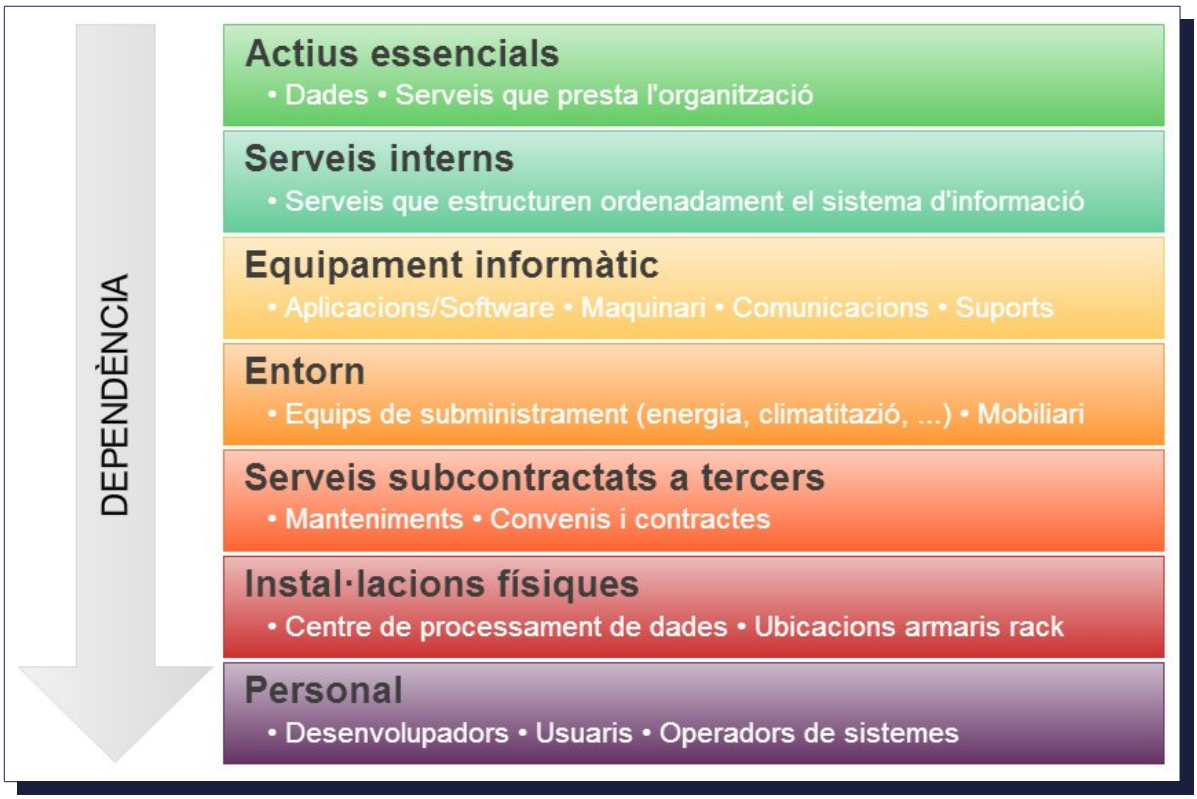

Figura 6-1: Esquema de capes de dependències segons Magerit.

En el nostre cas, considerarem que el Personal **[P]** i les Instal·lacions físiques **[L]** no tenen dependències inferiors. Per la resta caldrà analitzar-ho cas per cas, tenint en compte que la major part dels actius seguiran l'esquema que es mostra en la *Figura 6-1*.

La ***Taula 6-2*** de l'apartat **6.4** mostra un resum l'inventari d'actius, així com les seves relacions de dependència i classificació, juntament amb altres dades addicionals. Caldria elaborar una fitxa de dades per cadascun dels diferents elements, amb la seva descripció i dependències.

6.2 VALORACIÓ DELS ACTIUS

La metodologia Magerit precisa d'una valoració econòmica per cadascun dels actius. Aquesta valoració es pot consultar en l'apartat **5.6.5**. Per l'Ajuntament de Riberola, la valoració dels actius s'ha realitzat utilitzant les següents categories, corresponents a una valoració econòmica, tal i com s'aconsella a [**MAG2**, *Magerit Libro III - Técnicas*]:

- **[MA]** - Molt alt
- **[A]** - Alt
- **[M]** - Mig
- **[B]** - Baix
- **[MB]** - Molt Baix

Per realitzar una valoració correcta, cal programar entrevistes amb diferents departaments i responsables per tal de determinar el valor de cada element dins el conjunt de les funcions i processos de l'organització.

6.3 DIMENSIONS DE SEGURETAT

Per cada actiu caldrà analitzar la seva criticitat per l'organització en cadascuna de les cinc dimensions de seguretat següents [consultable en **MAG1**, *Apartat 3 - Dimensions de valoració*]:

- **[D] - Disponibilitat:** Propietat o característica dels actius consistent en que les entitats o processos autoritzats tenen accés als actius quan ho requereixen. Un actiu no té valor apreciable si pot romandre no disponible freqüentment o durant llargs períodes. Afecta a tot tipus d'actius.
- **[I] - Integritat de les dades:** característica que indicaria que l'actiu d'informació no ha estat alterat de manera no autoritzada. Si la seva alteració no suposa cap preocupació, el seu valor serà menyspreable.
- **[C] - Confidencialitat:** propietat consistent en que la informació ni es posa a disposició ni es revela a individus, entitats o processos no autoritzats. Si es valora que la revelació provocaria un greu perjudici a l'entitat o organització, obtindrà un valor alt.
- **[A] - Autenticitat:** propietat consistent en que una entitat, individu o procés és qui diu ser, o bé garanteix la font origen de les dades. Si un servei prestat a usuaris no autenticats pot provocar un greu perjudici, la dimensió d'autenticitat obtindrà un

valor alt. També pot ser-ho si el fet que la font origen de les dades és el que hauria pot provocar un perjudici greu.

- **[T] – Traçabilitat:** característica consistent en que les actuacions d'una entitat poden ser imputades a aquesta entitat o subjecte.

És molt important que l'escala de valoració de les diferents dimensions sigui la mateixa, per poder comparar-ne els riscos. Es pot optar per una valoració econòmica, que resulta molt complexa d'avaluar, o una de qualitativa, més senzilla però a l'hora més subjectiva i que permet valoracions a discreció de l'usuari. En aquest cas s'opta per aquesta última possibilitat, adaptant l'escala a la presentada per la metodologia Magerit:

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

Taula 6-1: Criteris de valoració del risc per les diferents dimensions

Tal i com es pot observar, l'escara és logarítmica, considerant el valor 0 com a risc menyspreable, i 10 com a risc extrem.

6.4 RESUM DE VALORACIÓ D'ACTIUS

Per la valoració pels diferents actius caldrà tenir en compte la seva relació jeràrquica amb els altres actius. Per tant, cada actiu disposarà d'un valor propi (el seu risc propi) i l'acumulat (valor màxim entre els actius superiors que depenen de l'actiu). Per tant, el valor acumulat serà calculat segons la fórmula [consultable en **MAG2**, anàlisi algorítmic del model quantitatiu]:

Sigui SUP(B) el conjunt d'actius superiors a B, és a dir, que depenen directa o indirectament de l'actiu B: $SUP(B) = \{ A_i, A_i \Rightarrow B \}$

Es defineix el valor acumulat sobre B com el valor major entre el propi de l'actiu B i el de qualsevol dels seus actius superiors:

$$valor\_acumulat(B) = max(valor(B), max_i\{valor(A_i)\})$$

Per tant, si per exemple disposem d'unes dades on la dimensió de disponibilitat rep una valoració de 9, i es recolza en un maquinari que en rebria 3, el maquinari passar a ser valorat en 9, ja que és necessària la seva disponibilitat degut a les dades que conté.

Respecte l'Esquema Nacional de Seguretat, cal considerar que caldria alinear els valors utilitzant una escala de Baix, Mitjà i Alt. Tot i així seria una conversió directa, assignant els valors Extrem, Molt Alt i Alt a Alt, Mitjà a Mitjà i Baix i Menyspreable a Baix.

En la següent taula (Taula 6-2) es presenta l'inventari dels actius, la seva classificació, relació jeràrquica, valoració per l'organització i valoració per les cinc dimensions de seguretat comentades en l'apartat anterior, amb els respectius valors acumulats:

[L] INSTAL·LACIONS

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[L.1]	CPD Casa Consistorial A	-	MA	-	-	10	-	-
[L.2]	CPD Casa Consistorial B	-	MA	-	-	10	-	-
[L.3]	CPD Secundari – Edifici Municipal	-	MA	-	-	10	-	-
[L.4]	CPD Centre Cívic	-	A	-	-	10	-	-
[L.5]	Armaris connexió de fibra òptica	-	A	-	-	10	-	-
[L.6]	Dependències i taller Departament TIC	-	M	-	-	9	-	-

[D] DADES

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[D.1]	Fitxers generals dels departaments	[SW.32],[HW.2], [Media2],[Media3]	A	4	8	6	7	6
[D.2]	Dades de padró	[SW.19],[HW.2]	MA	10	9	10	9	8
[D.3]	Registres d'entrada i sortida	[SW.19],[HW.2]	MA	9	9	9	8	6
[D.4]	Expedients	[SW.19],[HW.2]	MA	6	4	5	4	4
[D.5]	Recaptació – Gestió de tributs	[SW.19],[HW.2]	MA	9	10	9	8	9
[D.6]	Dades de comptabilitat/intervenció	[SW.20],[HW.2]	MA	8	6	9	6	6
[D.7]	Policia Local – Registres d'atenció telefònica	[SW.21],[HW.2]	M	9	10	6	3	7
[D.8]	Policia Local – Gestió actuacions i infraccions	[SW.21],[HW.2]	A	9	10	7	8	7
[D.9]	Dades personal, nòmines.	[SW.20],[HW.2]	MA	8	10	8	7	9
[D.10]	Correus electrònics i comptes	[SW.41],[HW.5]	A	7	9	6	7	8

[D.11]	Usuaris d'accés a xarxa i grups organitzatius	[SW.42],[HW.1]	MA	8	9	8	9	7
[D.12]	Incidències de les TIC	[SW.26],[HW.30]	M	2	6	3	2	2
[D.13]	Incidències Oficina Atenció Ciutadà	[SW.26],[HW.30]	B	0	2	0	0	2
[D.15]	Intranet corporativa	[SW.26],[HW.30]	B	2	3	1	1	2
[D.16]	Desenvolupaments aplicacions internes	[SW.32],[HW.2]	A	1	3	4	4	1
[D.17]	Registres de trucades i extensions telefòniques	[SW.39],[HW.4]	A	3	7	5	4	6
[D.18]	Gravacions de trucades emergències	[SW.13],[HW.4],[HW.6]	B	6	9	7	4	7
[D.19]	Gravacions de càmeres IP de dependències	[SW.43],[HW.6]	B	3	3	4	4	1
[D.20]	Dades de còpies de seguretat	[SW.33],[SW.34], [Media.1]	A	10	10	10	9	9

[K] CLAUS CRIPTOGRÀFIQUES

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[K.1]	Targetes criptogràfiques T-CAT personals	[P.1]	B	9	9	8	7	7
[K.2]	Certificats Fàbrica Nacional Moneda i Timbre	[SW.17]	B	7	7	2	4	1
[K.3]	Certificats de servidors (comunicacions SSL)	[SW.4],[SW.28]	B	8	7	7	8	7

[S] SERVEIS

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[S.1]	Controlador de domini primari / DNS / DHCP	[SW.1],[COM.12]	MA	9	9	9	10	8
[S.2]	Controlador de domini secundari	[SW.2],[COM.12]	B	9	8	9	1	8
[S.3]	Serveis d'impressió	[SW.6],[COM.12], [HW.28],[HW.29]	MB	3	6	3	2	2
[S.4]	Servidor de fitxers	[SW.32],[COM.12]	MA	4	8	6	7	6
[S.5]	Tràmits de gestió tributària	[SW.19],[COM.12]	MA	9	10	9	8	9
[S.6]	Pagaments i control pressupostari	[SW.20],[COM.12]	MA	8	6	9	6	6
[S.7]	Registre d'entrades i sortides	[SW.19],[COM.12]	MA	9	9	9	8	6
[S.8]	Control horari	[SW.23],[COM.12], [HW.32]	A	8	9	6	6	3
[S.9]	Gestió de nòmines i personal	[SW.20],[COM.12]	MA	8	10	8	7	9

[S.10]	Tràmits ciutadans online / inscripcions	[SW.19],[COM.4], [COM.12],[K.3]	A	8	7	6	8	7
[S.11]	Padró	[SW.19],[COM.12]	MA	10	9	10	9	8
[S.12]	Gestió d'expedients i òrgans col·legiats	[SW.19],[COM.12]	MA	6	4	5	4	4
[S.13]	Pagament infraccions	[SW.21],[COM.12]	MA	9	10	7	8	7
[S.15]	Comunicació administracions públiques / EACAT	[COM.4],[K.1],[COM.12]	M	7	8	8	4	6
[S.16]	Correu electrònic corporatiu	[SW.41],[COM.4], [COM.12]	A	7	9	6	7	8
[S.17]	Calendaris de coordinació departaments	[SW.22],[COM.12]	B	2	3	1	1	2
[S.18]	Web pública Ajuntament – Informació interès	[SW.29]	M	7	2	2	7	4
[S.19]	Altres webs secundàries	[COM.4],[SW.26], [SW.31]	B	7	2	2	4	2
[S.20]	Monitoratge d'elements i serveis TIC - Nagios	[SW.26],[COM.12], [COM.8]	A	3	6	4	2	2
[S.21]	Control accés internet i xarxa	[SW.40],[COM.12]	MA	5	9	8	8	7
[S.22]	IDS – Sistema de detecció d'intrusions	[SW.14],[COM.12]	MB	6	8	8	2	4
[S.23]	Consulta i gestió d'informes	[SW.25],[COM.12]	M	6	7	6	3	4
[S.24]	Enviament de SMS a ciutadans	[COM.4],[SW.26], [COM.12]	MB	7	0	0	2	1
[S.25]	Telefonia i gestió asterisk	[SW.39],[COM.12], [HW.23]	A	9	9	8	9	8
[S.26]	Cobrament de rebuts antics	[SW.38]	M	6	9	7	2	7
[S.27]	Perfil del contractant – Plataforma Gencat	[COM.4],[K.1]	A	7	1	7	7	7
[S.28]	Connexió a Internet – Organització	[S.21],[S.1],[COM.4], [COM.12]	A	4	9	7	6	6
[S.29]	Connexions WiFi públiques – Internet	[S.21],[COM.5], [COM.7],[COM.12]	MB	2	4	2	1	5
[S.30]	Gravació de càmeres de seguretat IP	[COM.12],[SW.43], [HW.25]	B	3	3	4	4	1
[S.31]	Control codi maliciós i virus	[SW.24]	M	8	8	8	5	6

[SW] APLICACIONS / SOFTWARE

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[SW.1]	S.O. Windows 2008 Server – DC01	[HW.1],[HW.11], [HW.12]	A	9	9	9	10	8
[SW.2]	S.O. Windows 2008 Server – DC02	[HW.10]	B	9	8	9	1	8
[SW.3]	S.O. Windows 2008 Server – NTSERVER-	[HW.1],[HW.11],	A	10	10	10	9	9

	NEW	[HW.12]						
[SW.4]	S.O. Windows 2008 Server – SRV2003R2-NEW	[HW.1],[HW.11], [HW.12]	A	10	10	10	9	9
[SW.5]	S.O. Windows 2000 Server	[HW.1],[HW.11], [HW.12]	M	0	0	7	2	1
[SW.6]	S.O. Windows 2003 Server (aoc)	[HW.1],[HW.11], [HW.12]	B	3	6	3	2	2
[SW.7]	S.O. Windows 2003 Server (backups-vmware)	[HW.13]	A	10	10	10	9	9
[SW.8]	S.O. Windows 2003 Server (backups)	[HW.3],[HW.31]	A	10	10	10	9	9
[SW.9]	S.O. Linux Ubuntu Server (varis)	[HW.30]	M	7	6	3	4	2
[SW.10]	S.O. Linux Ubuntu Server (proves)	[HW.9]	MB	7	6	3	4	2
[SW.11]	S.O. Linux Ubuntu Server (liferay)	[HW.1],[HW.11], [HW.12]	B	1	1	1	1	1
[SW.12]	S.O. Linux Ubuntu Server (jasper)	[HW.1],[HW.11], [HW.12]	B	6	7	6	3	4
[SW.13]	S.O. Linux Debian (VoIP)	[HW.4]	A	6	9	7	4	7
[SW.14]	S.O. Linux Ubuntu Server (IDS) Alienvault OSSIM	[HW.8]	B	6	8	8	2	4
[SW.15]	S.O. Linux Debian (tallafocs i proxy)	[HW.7]	M	5	9	8	8	7
[SW.16]	S.O. Linux Debian (correu)	[HW.5]	M	7	9	6	7	8
[SW.17]	S.S.O.O Estacions treball	[HW.21],[HW.22]	MB	7	8	7	4	5
[SW.18]	Aplicacions ofimàtiques	[HW.21],[HW.22]	B	0	0	3	2	0
[SW.19]	Aplicacions ABSIS	[SW.4],[SW.27],[SW.28]	A	10	10	10	9	9
[SW.20]	Aplicacions SIGEP/SICALWIN	[SW.3],[SW.27]	A	8	10	9	7	9
[SW.21]	Aplicacions GESPOL	[SW.4],[SW.27],[SW.28]	A	9	10	7	8	7
[SW.22]	Intranet corporativa	[HW.30]	MB	2	3	1	1	2
[SW.23]	Aplicació TEMPO	[SW.3],[SW.27]	A	8	9	6	6	3
[SW.24]	Antivirus – Estacions treball	[HW.21],[HW.22]	M	8	8	8	5	6
[SW.25]	Gestió informes – Jasper Reports / Jasper Server	[SW.12]	B	6	7	6	3	4
[SW.26]	Apache, PHP i MySQL	[SW.9],[SW.10]	B	7	6	3	4	2
[SW.27]	SQL Server 2008 R2	[SW.3],[SW.4]	M	10	10	10	9	9
[SW.28]	Internet Information Server	[SW.6],[SW.4]	M	10	10	10	9	9
[SW.29]	Plone – Allotjament extern	[COM.4],[HW.27]	M	7	2	2	7	4
[SW.30]	Connexió AOC-Padró – IIS	[COM.4],[SW.27], [SW.28]	B	7	8	7	3	4
[SW.31]	CMSs Joomla i Wordpress	[COM.4]	MB	7	2	2	4	2

[SW.32]	Compartició de fitxers	[SW.3]	A	4	8	6	7	6
[SW.33]	Veeam backup – Còpies d'imatges vmware	[COM.11],[SW.7], [HW.1],[HW.2]	A	10	10	10	9	9
[SW.34]	Backup Exec '12 – Gestió de cintes de backup	[SW.8]	A	10	10	10	9	9
[SW.35]	Autocad – Oficina tècnica	[HW.21]	B	2	0	7	4	2
[SW.36]	ITEC – Oficina Tècnica	[SW.5]	B	0	0	7	2	1
[SW.37]	Control dipòsits aigua i lectors contadors	[COM.10]	A	3	6	4	2	2
[SW.38]	Recaptació antiga – Rebuts pendents	[HW.24]	M	6	9	7	2	7
[SW.39]	Gestió de la telefonia IP	[SW.13],[COM.1], [COM.2],[COM.11], [HW.26]	A	9	9	8	9	8
[SW.40]	Tallafocs i proxies	[SW.15],[COM.11], [COM12]	A	5	9	8	8	7
[SW.41]	Correu corporatiu web	[SW.16]	M	7	9	6	7	8
[SW.42]	Gestió permisos i usuaris (Active Directory)	[SW.1]	A	8	9	8	9	7
[SW.43]	S.O. Linux Ubuntu – RAID (gravacions IP)	[HW.6]	B	3	3	4	4	1

[HW] MAQUINARI / HARDWARE

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[HW.1]	Cabina de discos SAS – S.S.O.O. Vmware	[AUX.1],[AUX.4], [AUX.7],[L.1]	MA	10	10	10	10	9
[HW.2]	Cabina de discos SATA – Dades	[AUX.1],[AUX.4], [AUX.7],[L.1]	MA	10	10	10	9	9
[HW.3]	Unitat robòtica de cintes de backup	[AUX.1],[AUX.4], [AUX.7],[L.1]	A	10	10	10	9	9
[HW.4]	Servidor clònic Asterisk VoIP	[AUX.2],[AUX.5], [AUX.7],[L.2]	A	6	9	7	4	7
[HW.5]	Servidor clònic Correu electrònic	[AUX.1],[AUX.4], [AUX.7],[L.1]	M	7	9	6	7	8
[HW.6]	Servidor clònic Enregistrament càmeres IP/VoIP	[AUX.1],[AUX.4], [AUX.7],[L.1]	B	6	9	7	4	7
[HW.7]	Servidor clònic Firewall	[AUX.1],[AUX.4], [AUX.7],[L.1]	A	5	9	8	8	7
[HW.8]	Servidor clònic IDS – Alienvault OSSIM	[AUX.1],[AUX.4],[L.1]	MB	6	8	8	2	4
[HW.9]	Servidor IBM Netfinity	[AUX.1],[AUX.4],[L.1]	MB	7	6	3	4	2
[HW.10]	Servidor HP Proliant – DC02	[L.6]	B	9	8	9	1	8
[HW.11]	HP Proliant G7 – VMWARE01	[AUX.1],[AUX.4], [AUX.7],[L.1]	MA	10	10	10	9	9

[HW.12]	HP Proliant G7 – VMWARE02	[AUX.1],[AUX.4], [AUX.7],[L.1]	MA	10	10	10	9	9
[HW.13]	HP Proliant G7 – VeeamBackup	[AUX.6],[AUX.3],[L.3]	A	10	10	10	9	9
[HW.14]	2 commutadors xarxa – VMWARE	[AUX.1],[AUX.4], [AUX.7],[L.1]	A	10	10	10	10	9
[HW.15]	Xassis xarxa – HP5412-CC	[AUX.2],[AUX.5], [AUX.7],[L.2]	MA	10	10	10	10	9
[HW.16]	Commutadors xarxa POE / VoIP (x3)	[AUX.2],[AUX.5], [AUX.7],[L.2]	A	10	10	10	10	9
[HW.17]	Commutadors xarxa nucli anella fibra NORTEL x3	[AUX.8],[L.2],[L.3], [L.4]	MA	10	10	10	10	9
[HW.18]	Anella fibra òptica (x18) – Switch ATI/HP	[AUX.8],[L.5]	A	10	10	10	10	9
[HW.19]	Xassis xarxa – HP5406-CPD Edifici secundari.	[AUX.6],[AUX.3],[L.3]	M	10	10	10	10	9
[HW.20]	Distribució xarxa edifici secundari (x7) HP	[AUX.9]	B	10	10	10	10	9
[HW.21]	Estacions de treball sobretaula	-	B	8	8	8	5	6
[HW.22]	Estacions de treball – Portàtils	-	B	8	8	8	5	6
[HW.23]	Terminals mòbils (telefonia i smartphones)	[P.1]	B	9	9	8	9	8
[HW.24]	AS/400 – Antiga recaptació	[AUX.1],[AUX.4],[L.1]	B	6	9	7	2	7
[HW.25]	Càmeres IP	-	MB	3	3	4	4	1
[HW.26]	Telèfons IP	-	B	9	9	8	9	8
[HW.27]	Allotjament web extern (lloguer de servidor)	-	A	7	2	2	7	4
[HW.28]	Parc Impressores pròpies	-	B	3	6	3	2	2
[HW.29]	Parc Impressores de rènting	-	B	3	6	3	2	2
[HW.30]	Servidor HP Proliant G5	[AUX.1],[AUX.4], [AUX.7],[L.1]	M	7	6	3	4	2
[HW.31]	Servidor IBM – Còpies Cintes	[AUX.1],[AUX.4], [AUX.7],[L.1]	A	10	10	10	9	9
[HW.32]	Terminals biomètrics – Fitxatges	-	B	8	9	6	6	3

[COM] COMUNICACIONS

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[COM.1]	Primari de teleonia fixa	[L.2]	MA	9	9	8	9	8
[COM.2]	Primari de telefonia mòbil	[L.2]	A	9	9	8	9	8
[COM.3]	RDSI Casa consistorial	[L.2]	MB	1	3	0	0	0
[COM.4]	ADSL primària 20Mb	[L.2]	A	8	9	8	8	8
[COM.5]	ADSL secundària 10Mb	-	M	2	4	2	1	5

[COM.7]	Routers WiFi – Internet	-	B	2	4	2	1	5
[COM.8]	Módem GSM – Alertes TIC	[L.1]	M	3	6	4	2	2
[COM.9]	Línies convencionals i FCT per alarmes	-	B	7	5	4	3	1
[COM.10]	Enllaç ràdio dipòsits aigua	[L.2]	A	3	6	4	2	2
[COM.11]	Xarxa de fibrà òptica municipal	[L.2],[L.3],[L.4], [HW.17],[HW.18]	MA	10	10	10	10	9
[COM.12]	Xarxa local organització (diverses VLANs)	[HW.14],[HW.15], [HW.16],[HW.17], [HW.18],[HW.19], [HW.20],[COM.11]	MA	10	10	10	10	9

[MEDIA] SUPORTS D'INFORMACIÓ

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[Media.1]	Cintes de còpies Backup	[L.7][HW.3][SW.34]	MA	10	10	10	9	9
[Media.2]	Memòries USB	[P.1]	M	4	8	6	7	6
[Media.3]	DVD, CD i disquets	[P.1]	M	4	8	6	7	6

[AUX] EQUIPAMENT AUXILIARS

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[AUX.1]	Refrigeració CPD-CC-A	[L.1]	B	-	-	10	10	-
[AUX.2]	Refrigeració CPD-CC-B	[L.2]	B	-	-	10	10	-
[AUX.3]	Refrigeració CPD Secundari	[L.3]	B	-	-	10	10	-
[AUX.4]	SAI CPD-CC-A	[L.1]	B	-	-	10	10	-
[AUX.5]	SAI-CPD-CC-B	[L.2]	B	-	-	10	10	-
[AUX.6]	SAI CPD Secundari	[L.3]	B	-	-	10	10	-
[AUX.7]	Armaris rack CPD	-	M	-	-	10	10	-
[AUX.8]	Armaris rack Anella fibra òptica	-	M	-	-	10	10	-
[AUX.9]	Armaris rack CPD Centre Cívic	[L.4]	B	-	-	10	10	-

[P] PERSONAL

CODI	ACTIU	DEPENDÈNCIES	VALOR	ASPECTES CRÍTICS				
				A	C	I	D	T
[P.1]	Usuaris	-		-	7	-	4	-

[P.2]	Administradors de sistemes i xarxes	-		-	10	-	10	-
[P.3]	Responsable de seguretat	-		-	10	-	10	-

Taula 6-2: Inventari, dependències i valoració d'actius

6.5 ANÀLISI D'AMENACES I IMPACTE POTENCIAL

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

Magerit, en el Llibre II, **[MAG1]**, ofereix la següent classificació amb les possibles amenaces que poden afectar els nostres actius, enumerant possibles amenaces per cadascuna:

- **[N] Desastres naturals:** successos que poden succeir sense intervenció humana.
- **[I] Amenaces d'origen industrial:** successos que poden ocórrer de manera accidental, derivats de l'activitat humana de tipus industrial.
- **[E] Errors i fallides no intencionades:** Erros no intencionats provocats per persones.
- **[A] Atacs intencionats:** Errors i fallides provocades deliberadament per persones.

Aquestes amenaces poden materialitzar-se amb una certa probabilitat, que ve definida per la següent taula de valors, on es veuen ocurrències per dies de l'any:

Valor		Criteri
1	1 cop al dia	Freqüència extrema
26/365 = 0,071	1 cop cada 2 setmanes	Freqüència alta
6/365 = 0,016	1 cop cada 2 mesos	Freqüència mitjana
2/365 = 0,005	1 cop cada 6 mesos	Freqüència baixa
1/365 = 0,002	1 cop l'any	Freqüència molt baixa

Taula 6-3: Probabilitats de materialització d'una amenaça

En Magerit, s'entén per impacte el tant per cent de valor que es perd de l'actiu en cas de materialitzar-se una amenaça concreta.

Per tant, cal considerar que si alguna amenaça es materialitza, es produirà un impacte en l'organització per alguna de les dimensions de l'actiu afectat. Aquests impactes potencials ens ajudaran a determinar quins actius de l'organització es veuen més afectats per les diferents

amenaces, tenint en compte la seva importància per l'organització.

La següent taula (*Taula 6-4*) presenta els diferents valors escollits per determinar el possible impacte de les amenaces sobre les diferents dimensions de cadascun dels actius:

Impacte	Valor
Molt alt	100%
Alt	75%
Mitjà	50%
Baix	20%
Molt baix	5%
Inexistent	0%

Taula 6-4: Possibles impactes sobre dimensions dels actius

Cal tenir en compte que sempre queda un impacte residual, ja que les amenaces sobre els actius es poden gestionar, però mai eliminar del tot el risc. Per tant, sempre existeix un possible impacte (tot i que molt reduït), a no ser que l'amenaça per la dimensió de l'actiu sigui impossible o completament inexistent per concepte.

A continuació, en la *Taula 6-5*, s'exposa un exemple de càlcul de les amenaces per uns grups d'actius. Degut a la seva extensió, el llistat complet de la taula d'amenaces per tots els actius numerats en la *Taula 6-2* es pot consultar en l'**Annex II** del present document. En la *Taula 6-5* d'exemple es pot comprovar com segons la tipologia i les característiques dels actius, els podem agrupar per calcular-ne les amenaces i la seva freqüència. També cal destacar que segons la classificació de l'actiu, les amenaces poden variar, ja que no són les mateixes per una localització que per una aplicació o un maquinari.

ACTIUS/AMENACES	FREQ.	A	C	I	D	T
[L.1],[L.2],[L.3],[L.4]		**0%**	**75%**	**75%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	50%	0%
[I] - DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,005	0%	0%	0%	50%	0%
[E] - ERRORS NO INTENCIONATS						
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	5%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	5%	0%	0%	0%
[A] - ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	5%	50%	50%	0%

[A.11] ACCÈS NO AUTORITZAT	0,016	0%	75%	75%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	20%	20%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
[A.27] OCUPACIÓ ENEMIGA	0,002	0%	75%	0%	75%	0%
[D.9],[D.10],[D.13],[D.15]		**100%**	**100%**	**100%**	**100%**	**20%**
[E] - ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	1	0%	20%	50%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,071	0%	50%	75%	20%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,016	0%	0%	5%	0%	20%
[E.4] ERRORS DE CONFIGURACIÓ	0,005	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A] - ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	5%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	20%	20%	5%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	75%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	100%	50%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	50%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[HW.21]		**0%**	**100%**	**50%**	**100%**	**0%**
[HW.22]		**0%**	**100%**	**50%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] - DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	50%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	50%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	75%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,002	0%	0%	0%	75%	0%
[E] - ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	5%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	20%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	100%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	50%	0%	100%	0%
[A] - ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	20%	20%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	20%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	50%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	75%	0%	20%	0%

[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%

Taula 6-5: Exemple d'amenaces

Per cada actiu i dimensió es considera el valor major calculat de les diferents amenaces. Degut a la complexitat del tractament de les dades, es aconsellable la utilització d'algun tipus de programari, com per exemple **EAR/PILAR**, gratuït per les administracions públiques espanyoles [**PIL0**]. Per tant, caldria considerar la introducció de les dades d'aquest projecte a l'eina en un futur per tal de facilitar-ne el manteniment i seguiment.

6.6 NIVELL DE RISC ACCEPTABLE I RISC RESIDUAL

Per tal de calcular el risc, tenir en compte principalment tres conceptes, el valor de l'actiu, la probabilitat que es produeixi una amenaça i l'impacte d'aquesta sobre l'actiu. En el nostre cas, al disposar d'un valor entre 0 i 10 per cadascuna de les dimensions, es realitzaran els següents càlculs per tal d'extreure el risc:

*Impacte [A,C,I,D,T] = Valor_actiu [A,C,I,D,T] * Degradació [A,C,I,D,T]*

*Risc [A,C,I,D,T] = Impacte [A,C,I,D,T] * Freqüència_amenaça*

Com que sortirà un risc per cada amenaça que afecta l'actiu, es considerarà només el màxim valor de risc per cadascuna de les dimensions. Amb aquest càlcul obtindrem quins són els actius més importants i exposats a amenaces dins la nostra organització.

En aquest punt cal tenir en compte que el rang de probabilitats que s'ha escollit per realitzar el projecte, proposat per Magerit, atorga molt pes a amenaces que se poden produir diàriament, mentre que al tenir en compte dies per any, els següents valor de risc es presentaran amb un valor bastant reduït.

Per poder identificar el risc de manera senzilla, identificarem els diferents riscs mitjançant zones, cadascuna amb un color. Aquestes zones vindran definides mitjançant la *Taula 6-6*:

Valor	
	Risc baix (< 0.15)
	Risc mitjà (>= 0.15 i < 0.5)
	Risc alt (>= 0.5 i 1.5)
	Risc molt alt (>= 1.5).

Taula 6-6: Resum colors risc

Degut a que s'ha considerat la probabilitat de les amenaces emprant una escala logarítmica, el risc de cada actiu ve definit per una gràfica del tipus que s'observa a la *Figura 6-2* (corbes logarítmiques). En aquesta gràfica es pot observar com el risc d'un actiu ve definit per la combinació entre la probabilitat de materialització d'una amenaça, amb l'impacte que tindria la pèrdua de l'actiu per l'organització. Si un actiu provoca un impacte menyspreable, per molt que pugui patir la materialització d'una amenaça força sovint, el risc quedarà en la zona baixa. De la mateixa manera, si una amenaça té una probabilitat de materialització mínima, per molt impacte que suposi per l'organització també obtindrà un valor de risc baix.

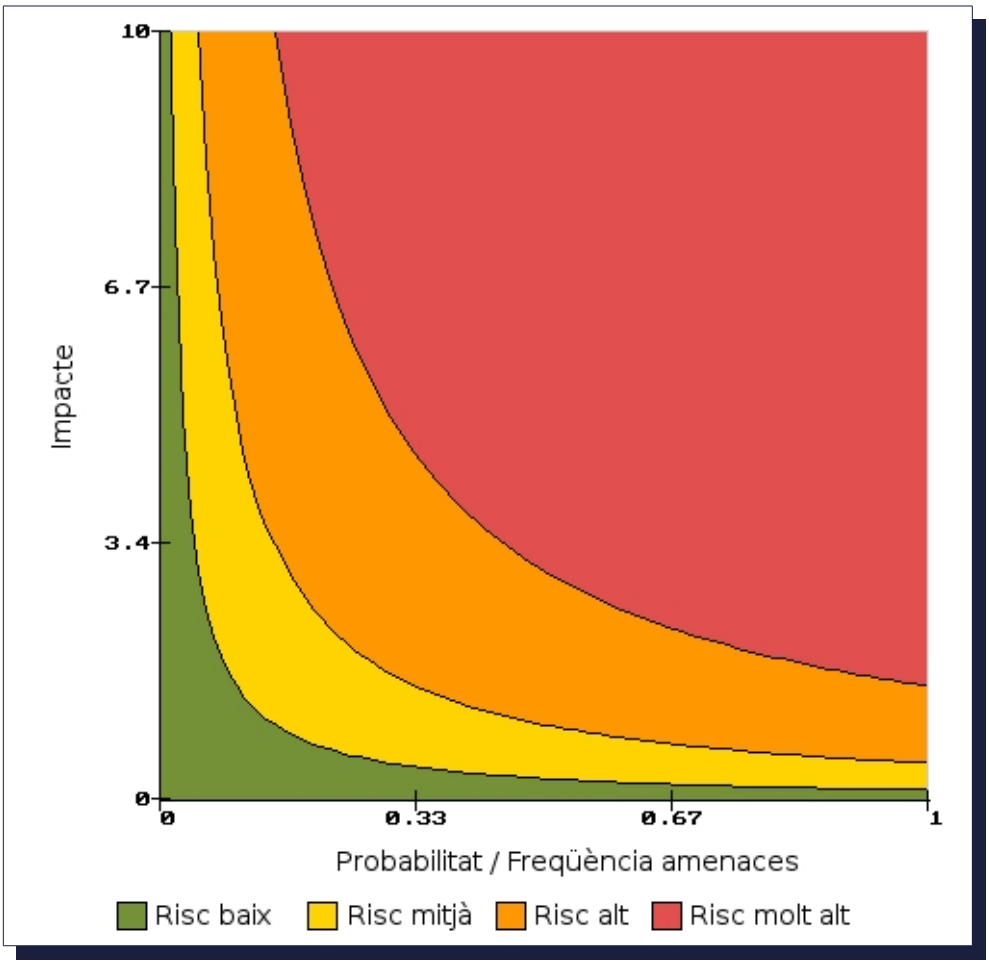

Figura 6-2: Gràfica probabilitat d'amenaça per Impacte pels actius.

Per tant, l'organització prioritzarà els riscos segons la taula i gràfica anteriors (*Taula 6-6* i *Figura 6-2*), definint com a risc acceptable aquell que té valor baix (per sota de 0.15), i que per tant es manté en la zona de risc baix. Ubicar els diferents actius dins d'una gràfica del tipus de la *Figura 6-2* ajudarà a saber si el risc d'un actiu és degut al seu impacte o més aviat per la probabilitat de materialització d'alguna amenaça.

A continuació es presenten les següents taules amb els valors de risc calculats segons els paràmetres comentats anteriorment.

6.6.1 INSTAL·LACIONS

CODI	DESCRIPCIÓ	A	C	I	D	T
[L.1]	CPD Casa Consistorial A	0	0	0,12	0	0
[L.2]	CPD Casa Consistorial B	0	0	0,12	0	0
[L.3]	CPD Secundari - Edifici Municipal	0	0	0,12	0	0
[L.4]	CPD Centre Cívic	0	0	0,12	0	0
[L.5]	Armaris connexió fibra òptica	0	0	0,032	0	0
[L.6]	Dependències i taller TIC	0	0	0,108	0	0

Taula 6-7: Risc instal·lacions

6.6.2 DADES

CODI	DESCRIPCIÓ	A	C	I	D	T
[D.1]	Fitxers generals dels departaments	0,02	0,128	0,096	0,035	0,015
[D.2]	Dades de padró	0,05	0,144	0,16	0,045	0,02
[D.3]	Registres d'entrada i sortida	0,045	0,144	0,144	0,04	0,015
[D.4]	Expedients	0,03	0,064	0,08	0,02	0,01
[D.5]	Recaptació - Gestió de tributs	0,045	0,16	0,144	0,04	0,0225
[D.6]	Dades de comptabilitat/intervenció	0,04	0,096	0,144	0,0225	0,015
[D.7]	Policia Local - Registres d'atenció telefònica	0,045	0,16	0,096	0,015	0,0175
[D.8]	Policia Local - Gestió actuacions i infraccions	0,045	0,16	0,112	0,04	0,0175
[D.9]	Dades personal, nòmines.	0,016	2	4	0,35	0,0288
[D.10]	Correus electrònics i comptes	0,014	1,8	3	0,35	0,0256
[D.11]	Usuaris d'accés a xarxa i grups organitzatius	0,008	0,108	0,064	0,108	0,0105
[D.12]	Incidències de les TIC	0,002	0,072	0,024	0,024	0,003
[D.13]	Incidències Oficina Atenció Ciutadà	0	0,4	0	0	0,0064
[D.15]	Intranet corporativa	0,004	0,6	0,5	0,05	0,0064
[D.16]	Desenvolupaments aplicacions internes	0,001	0,0075	0,048	0,01	0,0004
[D.17]	Registres de trucades i extensions	0,0012	0,035	0,06	0,032	0,072

	telefòniques					
[D.18]	Gravacions de trucades emergències	0,0024	0,045	0,084	0,032	0,084
[D.19]	Gravacions de càmeres IP de dependències	0,0012	0,015	0,048	0,032	0,012
[D.20]	Dades Còpies de seguretat	0,015	0,032	0,355	0,639	0,47925

Taula 6-8: Risc dades

6.6.3 CLAUS CRIPTOGRÀFIQUES

CODI	DESCRIPCIÓ	A	C	I	D	T
[K.1]	Targetes criptogràfiques T-CAT personals	0,47925	0,016	0,0284	0,02485	0
[K.2]	Certificats Fàbrica Nacional Moneda i Timbre	0,112	0,112	0,0016	0,048	0
[K.3]	Certificats de servidors (comunicacions SSL)	0,016	0,0105	0,007	0,04	0

Taula 6-9: Risc claus criptogràfiques

6.6.4 SERVEIS

CODI	DESCRIPCIÓ	A	C	I	D	T
[S.1]	Controlador de domini primari / DNS / DHCP	0,0135	0,108	0,108	0,16	0,0032
[S.2]	Controlador de domini secundari	0,0135	0,096	0,108	0,016	0,0032
[S.3]	Serveis d'impressió	0,0045	0,072	0,036	0,032	0,0008
[S.4]	Servidor de fitxers	0,006	0,096	0,072	0,112	0,0024
[S.5]	Tràmits de gestió tributària	0,018	0,05	0,3195	0,128	0,0036
[S.6]	Pagaments i control pressupostari	0,016	0,03	0,3195	0,096	0,0024
[S.7]	Registre d'entrades i sortides	0,018	0,045	0,3195	0,128	0,0024
[S.8]	Control horari	0,012	0,108	0,072	0,096	0,0012
[S.9]	Gestió de nòmines i personal	0,012	0,12	0,096	0,112	0,0036
[S.10]	Tràmits ciutadans online / inscripcions	0,016	0,035	0,213	0,128	0,0028
[S.11]	Padró	0,02	0,045	0,355	0,144	0,0032
[S.12]	Gestió d'expedients i òrgans col·legiats	0,012	0,02	0,1775	0,064	0,0016
[S.13]	Pagament infraccions	0,018	0,05	0,2485	0,128	0,0028

[S.15]	Comunicació administracions públiques	0,0105	0,0256	0,1136	0,048	0,009
[S.16]	Correu electrònic corporatiu	0,014	0,639	0,0852	0,112	0,0032
[S.17]	Calendaris de coordinació departaments	0,003	0,036	0,012	0,016	0,0008
[S.18]	Web pública Ajuntament - Informació interès	0,014	0,142	0,0284	0,112	0,0016
[S.19]	Altres webs secundàries	0,014	0,142	0,0284	0,064	0,0008
[S.20]	Monitoratge d'elements i serveis TIC - Nagios	0,0045	0,072	0,048	0,032	0,0008
[S.21]	Control accés internet i xarxa	0,0075	0,108	0,096	0,128	0,0028
[S.22]	IDS - Sistema de detecció d'intrusions	0,009	0,096	0,096	0,032	0,0016
[S.23]	Consulta i gestió d'informes	0,009	0,084	0,072	0,048	0,0016
[S.24]	Enviament de SMS a ciutadans	0,014	0	0	0,032	0,0004
[S.25]	Telefonia i gestió asterisk	0,018	0,639	0,1136	0,144	0,0032
[S.26]	Cobrament de rebuts antics	0,012	0,045	0,2485	0,032	0,0028
[S.27]	Perfil del contractant - Plataforma Gencat	0,014	0,071	0,0994	0,112	0,0028
[S.28]	Connexió a Internet - Organització	0,008	0,639	0,0994	0,096	0,0024
[S.29]	Connexions WiFi públiques - Internet	0,004	0,284	0,0284	0,016	0,002
[S.30]	Gravació de càmeres de seguretat	0,003	0,01125	0,0142	0,032	0,0001
[S.31]	Control codi maliciós	0,012	0,096	0,096	0,08	0,0024

Taula 6-10: Risc serveis

6.6.5 APLICACIONS I PROGRAMARI

CODI	DESCRIPCIÓ	A	C	I	D	T
[SW.1]	S.O. Windows 2008 Server	0,045	4,5	4,5	7,5	0,008
[SW.2]	S.O. Windows 2008 Server	0,045	4	4,5	0,75	0,008
[SW.3]	S.O. Windows 2008 Server	0,05	5	5	6,75	0,009
[SW.4]	S.O. Windows 2008 Server	0,05	5	5	6,75	0,009
[SW.5]	S.O. Windows 2000 Server	0	0	3,5	1,5	0,001
[SW.6]	S.O. Windows 2003 Server (aoc)	0,015	3	1,5	1,5	0,002
[SW.7]	S.O. Windows 2003 Server (backups-vmware)	0,05	5	5	6,75	0,009
[SW.8]	S.O. Windows 2003 Server (backups)	0,05	5	5	6,75	0,009
[SW.9]	S.O. Linux Ubuntu Server (varis)	0,035	3	1,5	3	0,002

[SW.10]	S.O. Linux Ubuntu Server (proves)	0,035	3	1,5	3	0,002
[SW.11]	S.O. Linux Ubuntu Server (liferay)	0,005	0,5	0,5	0,75	0,001
[SW.12]	S.O. Linux Ubuntu Server (jasper)	0,03	3,5	3	2,25	0,004
[SW.13]	S.O. Linux Debian (VoIP)	0,03	4,5	3,5	3	0,007
[SW.14]	S.O. Linux Ubuntu Server (IDS)	0,03	4	4	1,5	0,004
[SW.15]	S.O. Linux Debian (tallafocs i proxy)	0,025	4,5	4	6	0,007
[SW.16]	S.O. Linux Debian (correu)	0,035	4,5	3	5,25	0,008
[SW.17]	S.S.O.O Estacions treball	0,035	4	3,5	3	0,005
[SW.18]	Aplicacions ofimàtiques	0	0	0,15975	0,142	0
[SW.19]	Aplicacions ABSIS	0,05	0,142	0,5325	0,639	0
[SW.20]	Aplicacions SIGEP/SICALWIN	0,04	0,142	0,47925	0,497	0
[SW.21]	Aplicacions GESPOL	0,045	0,142	0,37275	0,568	0
[SW.22]	Intranet corporativa	0,01	0,0426	0,05325	0,071	0
[SW.23]	Aplicació TEMPO	0,04	0,1278	0,3195	0,426	0
[SW.24]	Antivirus - Estacions treball	0,012	0,1136	0,0284	0,1775	0
[SW.25]	Gestió informes - Jasper Server	0,03	0,0994	0,3195	0,213	0
[SW.26]	Apache, PHP i MySQL	0,0105	0,0852	0,01065	0,142	0
[SW.27]	SQL Server 2008 R2	0,015	0,142	0,0355	0,3195	0
[SW.28]	Internet Information Server	0,015	0,142	0,0355	0,3195	0
[SW.29]	Plone - Allotjament extern	0,056	0,071	0,1065	0,497	0
[SW.30]	Connexió AOC-Padró - IIS	0,056	0,284	0,37275	0,213	0
[SW.31]	CMSs Joomla i Wordpress	0,056	0,071	0,1065	0,284	0
[SW.32]	Compartició de fitxers	0,02	0,1136	0,3195	0,497	0
[SW.33]	Veeam backup - Còpies d'imatges vmware	0,01	0,02	0,12	0,639	0
[SW.34]	Backup Exec '12 - Gestió de cintes de backup	0,01	0,02	0,12	0,639	0
[SW.35]	Autocad - Oficina tècnica	0,01	0	0,37275	0,284	0
[SW.36]	ITEC - Oficina Tècnica	0	0	0,37275	0,142	0
[SW.37]	Control dipòsits aigua i lectors contadors	0,015	0,0852	0,213	0,142	0
[SW.38]	Recaptació antiga - Rebuts pendents	0,03	0,1278	0,37275	0,142	0
[SW.39]	Gestió de la telefonia IP	0,072	0,3195	0,426	0,639	0
[SW.40]	Tallafocs i proxies	0,04	0,3195	0,426	0,568	0
[SW.41]	Correu corporatiu web	0,056	0,3195	0,3195	0,497	0
[SW.42]	Gestió permisos i usuaris (Active Directory)	0,012	0,1278	0,0284	0,3195	0

Taula 6-10: Risc d'actiu d'aplicacions

6.6.6 MAQUINARI O HARDWARE

CODI	DESCRIPCIÓ	A	C	I	D	T
[HW.1]	Cabina de discos SAS - S.S.O.O.	0	0,02	0,02	0,71	0

	Vmware					
[HW.2]	Cabina de discos SATA - Dades	0	0,02	0,02	0,639	0
[HW.3]	Unitat robòtica de cintes de backup	0	0,02	0,032	0,3195	0
[HW.4]	Servidor clònic Asterisk VoIP	0	0,0135	0,056	0,284	0
[HW.5]	Servidor clònic Correu electrònic	0	0,0135	0,048	0,497	0
[HW.6]	Servidor clònic Enregistrament càmeres IP/VoIP	0	0,0135	0,056	0,284	0
[HW.7]	Servidor clònic Firewall	0	0,0135	0,064	0,568	0
[HW.8]	Servidor clònic IDS - Alienvault OSSIM	0	0,012	0,064	0,142	0
[HW.9]	Servidor IBM Netfinity	0	0,009	0,024	0,284	0
[HW.10]	Servidor HP Proliant - DC02	0	0,012	0,072	0,071	0
[HW.11]	HP Proliant G7 - VMWARE01	0	0,015	0,08	0,639	0
[HW.12]	HP Proliant G7 - VMWARE02	0	0,015	0,08	0,639	0
[HW.13]	HP Proliant G7 - VeeamBackup	0	0,015	0,08	0,639	0
[HW.14]	2 commutadors xarxa - VMWARE	0	0,025	0,015	0,71	0
[HW.15]	Xassis xarxa - HP5412-CC	0	0,025	0,015	0,71	0
[HW.16]	Commutadors xarxa POE / VoIP	0	0,025	0,015	0,71	0
[HW.17]	Commutadors xarxa nucli anella fibra NORTEL	0	0,025	0,015	0,71	0
[HW.18]	Anella fibra òptica (x18) - Switch ATI/HP	0	0,025	0,015	0,71	0
[HW.19]	Xassis xarxa - HP5406-CPD Edifici secundari.	0	0,025	0,015	0,71	0
[HW.20]	Distribució xarxa edifici secundari (x7) HP	0	0,025	0,015	0,71	0
[HW.21]	Estacions de treball fixes	0	0,016	0,008	0,1775	0
[HW.22]	Estacions de treball mòbils	0	0,016	0,008	0,1775	0
[HW.23]	Terminals mòbils (telefonia i smartphones)	0	0,108	0,008	0,144	0
[HW.24]	AS/400 - Antiga recaptació	0	0,0135	0,056	0,142	0
[HW.25]	Càmeres IP	0	0,108	0,008	0,144	0
[HW.26]	Telèfons IP	0	0,024	0,002	0,112	0
[HW.27]	Allotjament web extern (lloguer de servidor)	0	0,003	0,016	0,497	0
[HW.28]	Parc Impressores pròpies	0	0,0048	0,0024	0,1065	0
[HW.29]	Parc Impressores de rènting	0	0,0048	0,0024	0,1065	0
[HW.30]	Servidor HP Proliant G5	0	0,009	0,024	0,284	0
[HW.31]	Servidor IBM - Còpies Cintes	0	0,015	0,08	0,639	0

[HW.32]	Terminals biomètrics – Fitxatges	0	0,108	0,006	0,096	0

Taula 6-11: Risc dels actius de maquinari

6.6.7 COMUNICACIONS

CODI	DESCRIPCIÓ	A	C	I	D	T
[COM.1]	Primari de teleonia fixa	0	0,03375	0,016	0,045	0
[COM.2]	Primari de telefonia mòbil	0	0,03375	0,016	0,045	0
[COM.3]	RDSI Casa consistorial	0	0,01125	0	0	0
[COM.4]	ADSL primària 20Mb	0	0,03375	0,016	0,04	0
[COM.5]	ADSL secundària 10Mb	0	0,015	0,004	0,005	0
[COM.7]	Xarxes WiFi	0,002	0,0128	0,0064	0,071	0
[COM.8]	Módem GSM – Alertes TIC	0	0,01875	0,008	0,015	0
[COM.9]	Línies convencionals i FCT per alarmes	0	0,0225	0,008	0,01	0
[COM.10]	Enllaç ràdio dipòsits aigua	0	0,0375	0,02	0,05	0
[COM.11]	Xarxa de fibrà òptica municipal	0,02	0,12	0,032	0,16	0
[COM.12]	Xarxa local organització (diverses VLANs)	0,02	0,12	0,032	0,16	0

Taula 6-12: Risc dels actius de comunicacions

6.6.8 SUPORTS D'INFORMACIÓ

CODI	DESCRIPCIÓ	A	C	I	D	T
[Media.1]	Cintes backup	0	0,08	0,12	0,144	0
[Media.2]	Memòries USB	0	0,128	0,096	0,112	0
[Media.3]	DVD, CD i disquets	0	0,128	0,096	0,112	0

Taula 6-13: Risc dels suports d'informació

6.6.9 EQUIPAMENTS AUXILIARS

CODI	DESCRIPCIÓ	A	C	I	D	T
[AUX.1]	Refrigeració CPD-CC-A	0	0	0,01	0,355	0
[AUX.2]	Refrigeració CPD-CC-B	0	0	0,01	0,355	0
[AUX.3]	Refrigeració CPD Secundari	0	0	0,01	0,355	0
[AUX.4]	SAI CPD-CC-A	0	0	0,015	0,355	0
[AUX.5]	SAI-CPD-CC-B	0	0	0,015	0,355	0

[AUX.6]	SAI CPD Secundari	0	0	0,015	0,355	0
[AUX.7]	Armaris rack CPD	0	0	0	0,02	0
[AUX.8]	Armaris rack Anella fibra òptica	0	0	0	0,02	0
[AUX.9]	Armaris rack CPD Centre Cívic	0	0	0	0,02	0

Taula 6-14: Risc dels equipaments auxiliars

6.6.10 PERSONAL

CODI	DESCRIPCIÓ	A	C	I	D	T
[P.1]	Usuaris	0	0,112	0	0	0
[P.2]	Administradors de sistemes i xarxes	0	0,16	0	0,71	0
[P.3]	Responsable de seguretat	0	0,16	0	0,71	0

Taula 6-15: Risc del personal

6.7 SÍNTESI DELS RESULTATS OBTINGUTS

Durant aquesta fase s'ha realitzat un anàlisi exhaustiu dels diferents actius de l'organització, així com una valoració d'aquests actius per cadascuna de les diferents dimensions (autenticitat, confidencialitat, integritat, disponibilitat i traçabilitat). A més, en aquesta relació (*Taula 6-2*), s'hi mostren les relacions de dependència entre els actius, de manera que la importància d'un actiu superior es veu reflectida en els seus actius inferiors.

Mitjançant el resultat d'aquest anàlisi inicial dels actius se'n poden treure certes conclusions:

- L'organització determina que els serveis que s'ofereixen al ciutadà són crítics pel funcionament de l'organització.
- Els actius que permeten el funcionament correcte d'aquests serveis veuen reflectit en el seu valor aquesta relació de dependència.
- Es valora en menor mesura altres funcionalitats vinculades a gestió interna i relació amb altres administracions.

Fent ús d'aquest anàlisi d'actius, i fent ús dels paràmetres definits en l'apartat 5.6.7 del present document, es relaciona cada tipus d'actiu amb un conjunt de possibles amenaces que Magerit ofereix com a guia. Per cada amenaça se'n calcula una probabilitat que succeeixi, així com l'impacte que tindria per l'organització en cas de succeir.

Un cop realitzat el càlcul de l'impacte, es relaciona amb el valor per cadascuna de les dimensions, donant lloc a una taula de riscs dels actius, que es pot consultar en l'apartat 6.6.

L'anàlisi d'aquesta taula permet extreure els actius que tenen més risc i que a l'hora són crítics per l'organització.

En la *Figura 6-3* podem observar els 10 actius o conjunt d'actius que presenten un risc més elevat:

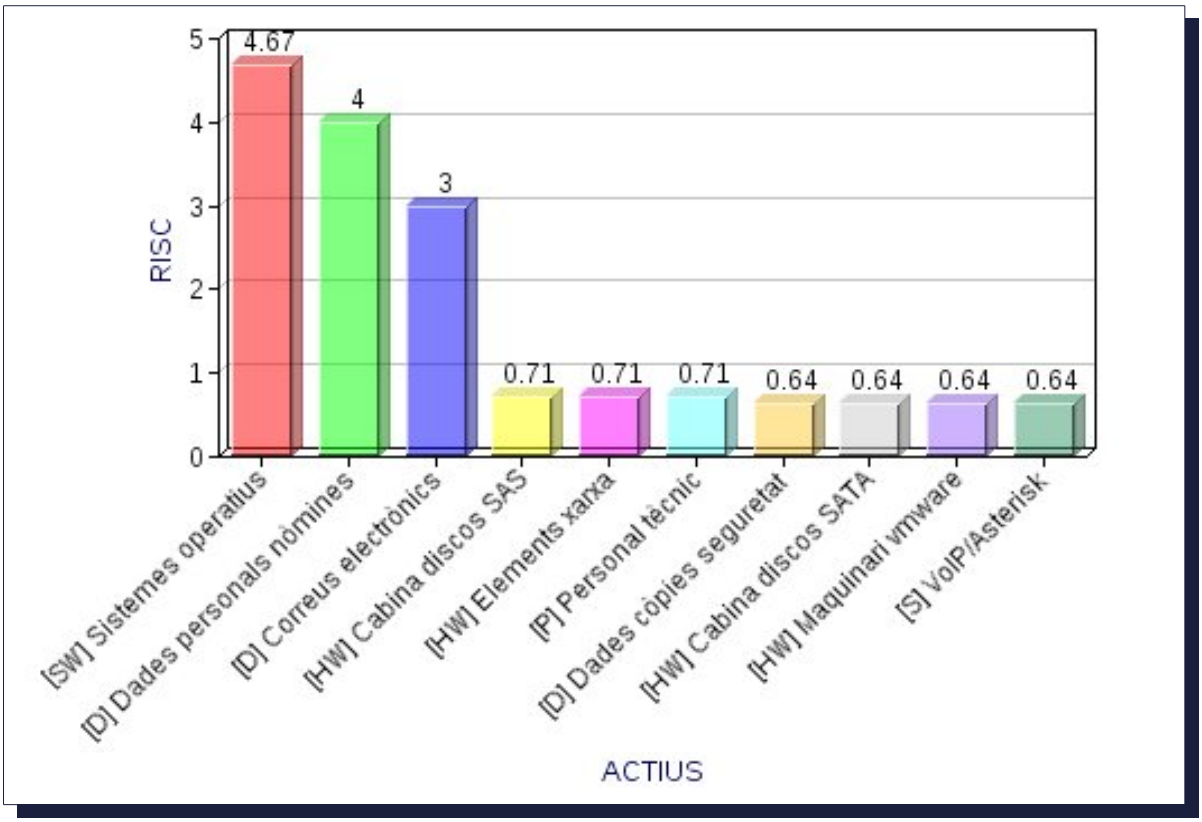

Figura 6-3: Conjunts d'actius amb risc més elevat

Agafant d'aquests actius, la dimensió amb més risc, podem realitzar una gràfica similar a la *Figura 6-2*, aquest cop ubicant els 10 actius amb més risc. El resultat es pot observar en la *Figura 6-4*. En aquest cas, la gràfica ens mostra clarament si els actius estan en risc per la probabilitat, per l'impacte o pels dos elements a la vegada. Per exemple, agafant l'actiu [SW-1] com exemple dels sistemes operatius, es pot observar com l'impacte no és tot l'elevat que podria ser, però es combina amb una probabilitat molt alta. El mateix cas succeeix amb els actius de dades [D-9] i [D-10], l'impacte encara és menor que en el primer cas, però la probabilitat o freqüència de materialització de l'amenaça és màxima. Per tant, el risc obtingut per aquestes tres elements és molt alt, i estan en la zona vermella de la gràfica. D'altra banda, altres elements que ja mostren un risc inferior en la Taula 6-3 es pot veure que la probabilitat s'ha reduït molt, tot i que l'impacte entre 9 i 10 provoca que els actius presentin un risc alt. Finalment, s'han afegit a la gràfica dos actius que presenten un risc inferiors, en concret els [HW-21] estacions de treball i els [COM-7] xarxes wifi. Aquests dos actius representen un impacte molt menor per l'organització, i la probabilitat no és massa

elevada, per tant, presenten un risc mitjà i baix respectivament.

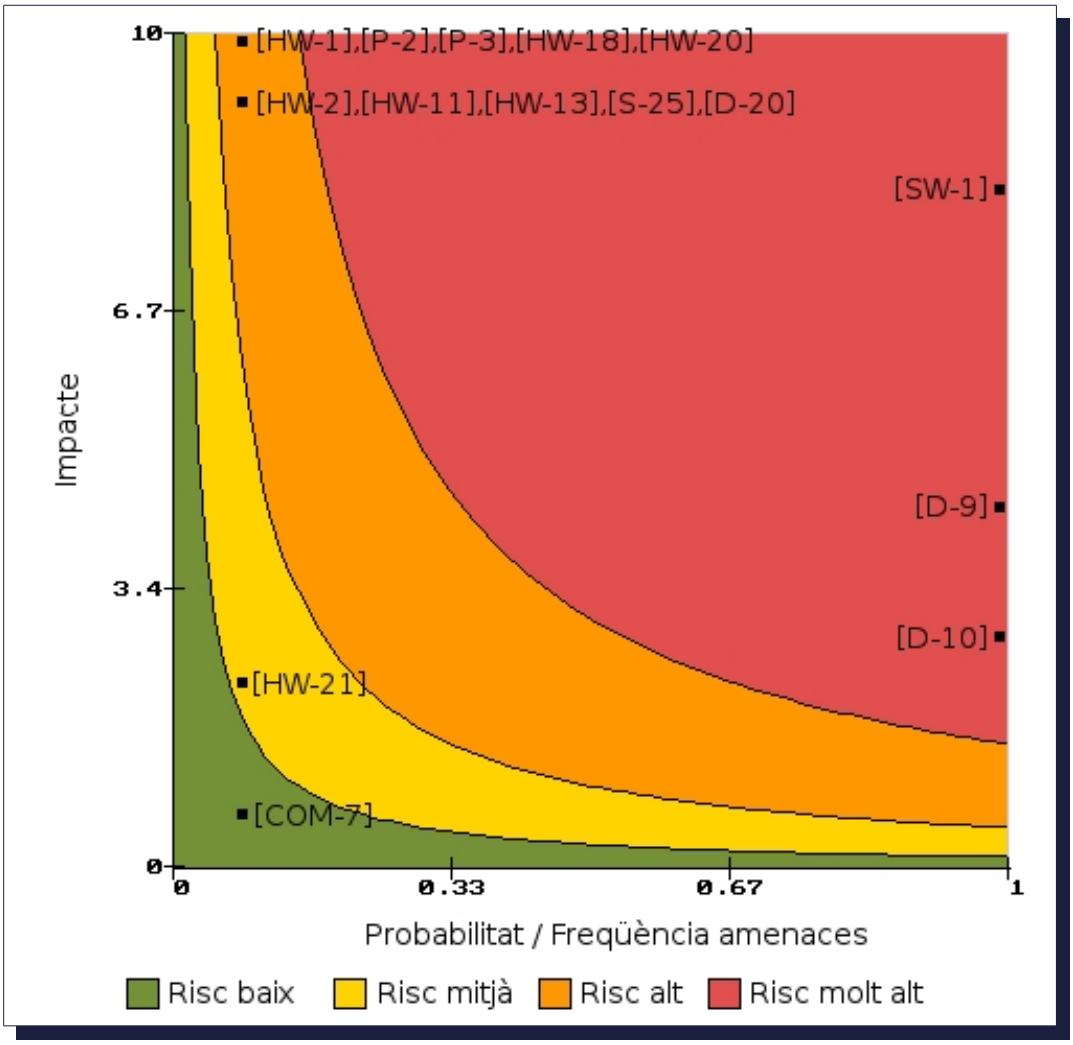

Figura 6-4: Representació dels actius amb més risc dins de gràfica impacte x freq.

També és interessant observar la *Figura 6-5* i la *Taula 6-16*, on es mostren les amenaces més probables i el conjunt d'actius als que afecta aquesta màxima probabilitat:

AMENAÇA	FREQ.	ACTIUS
[E.8] DIFUSIÓ DE MALWARE	1	[SW]
[E.1] ERRORS D'USUARI	0,071	[SW,S K]
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,071	[SW,S]
[E.2] ERRORS DE L'ADMINISTRADOR	0,071	[SW,D]
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,071	[SW]
[A.7] ÚS NO PREVIST	0,071	[SW]

[E.10] ERRORS DE SEQÜÈNCIA	0,071	[S]
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,071	[S]
[E.28] INDISPONIBILITAT DEL PERSONAL	0,071	[P]
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	[HW]
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,071	[HW]
[E.3] ERRORS DE MONITORITZACIÓ	0,071	[D]
[I.1] FALLADA SERVEI COMUNICACIONS	0,071	[COM]
[E.23] ERRORS DE MANTENIMENT/ACTUALITZACIÓ	0,071	[AUX,SW]
[A.11] ACCÈS NO AUTORITZAT	0,016	[SW,L,K]

Taula 6-16: Amenaces més probables

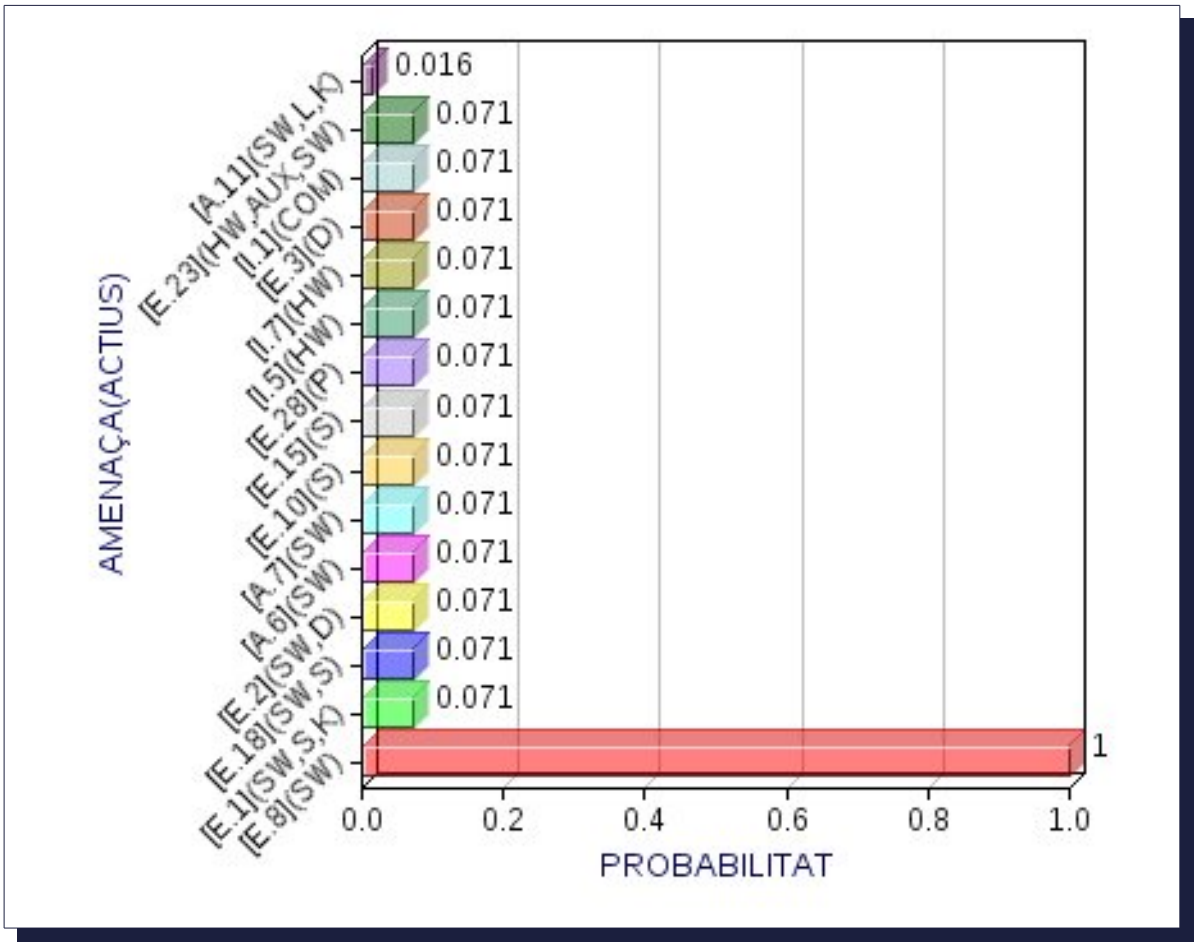

Figura 6-5: Amenaces més probables i conjunt d'actius afectats

Si realitzem el seguiment dels diferents resultats obtinguts, en general podem observar els següents punts a tenir en compte:

- Els actius que formen part del conjunt de les **instal·lacions [L]** presenten un risc que l'organització considera assumible.
- En els **actius de dades [D]** es presenten diversos actius amb risc, fent especial incís en les dades de personal [D.9] i correu electrònic [D.10], on es presenta un rics crític en els dominis de confidencialitat i integritat de les dades. Si observem els actius de dades en l'annex II, es pot comprovar que l'origen d'aquest risc són errors d'usuaris i d'administració. Pot ser degut a ineficàcia dels processos inferiors (o aplicacions) o a falta de formació del personal. És clar que degut a la importància de l'actiu és un punt a tractar. També cal destacar un compromís en la gestió del risc de les dades de la intranet de l'organització [D.15], en els dominis de confidencialitat i integritat, per la mateixa raó que els actius anteriors, però amb menor risc degut al seu menor valor.
- Els actius de **claus criptogràfiques [K]** presenten un actiu, el [K.1], targetes criptogràfiques T-CAT, que presenta un risc mitjà en la dimensió d'autenticitat. Això és degut a que certes targetes les utilitza a la pràctica més d'una persona, quan en realitat són intransferibles.
- Els **actius de serveis [S]** no contenen cap actiu en situació de risc molt alt, tot i que apareixen tres casos amb risc mitjà: correu electrònic corporatiu [S.16], telefonia i gestió de centraleta [S.25] i connexió a Internet [S.28]. Aquests tres serveis presenten un risc alt en la dimensió de confidencialitat. En el llistat d'amenaces de l'Annex II es pot observar que es presenta un risc alt per l'alta probabilitat d'errors d'usuari.
- En les **aplicacions [SW]** se'ns presenten diversos riscos, però destaquen de manera important els riscos crítics que presenten els Sistemes Operatius en el seu conjunt, ja siguin de servidors com d'estacions de treball. Aquests actius presenten una alta valoració degut als serveis i aplicacions als que donen servei, però a més es veuen afectats per una amenaça de difusió de malware, la qual es produeix amb una periodicitat diària. Aquest fet és degut a la manca d'aplicacions antivirus als servidors, a més de la manca d'actualització i poca centralització del servei d'antivirus de les estacions de treball. També s'hi poden observar riscos provinents d'altres amenaces com destrucció i alteració de la informació, així com errors de manteniment i actualitzacions. Per tant, l'organització hauria de posar els mitjans necessaris per realitzar la gestió d'aquests riscos el més aviat possible. Els altres riscos d'aplicacions afectes la dimensió de disponibilitat de les aplicacions, i caldria veure'n particularment cadascun dels casos.
- En el **maquinari [HW]** destaquen certs elements on la disponibilitat presenta un risc alt. Analitzant la taula d'amenaces per aquests actius podem determinar que la causa

és una amenaça degut a condicions inadequades de temperatura. Caldrà revisar, per part de l'organització, els equips de refrigeració de les sales o localitzacions dels diferents actius afectats.

- En referència als actius de **comunicacions [COM]**, només cal destacar un risc mitjà en la disponibilitat de la xarxa local i la xarxa de fibra òptica. Donat els elements que precisen d'aquestes dos xarxes per prestar els serveis de l'organització, són dos actius de vital importància. Aquest risc en la disponibilitat ve determinat per una freqüència no massa alta de fallada en les comunicacions, però que degut a la importància de l'actiu implica un augment del risc.
- La gestió dels **mitjans extraïbles [Media]** sembla estar ben gestionada degut a que els riscos que presenten els seus actius estan dins del rang de riscos assumibles per part de l'organització.
- En els **equips auxiliar [AUX]** destaquen, en disponibilitat, dos grups d'actius, els equips de refrigeració i els sistemes d'alimentació ininterrompuda. Els dos presenten un risc elevat per l'alta probabilitat i impacte d'un possible tall elèctric o danys per aigua.
- Finalment cal considerar els actius de **personal [P]**. Fent un anàlisi dels riscos, podem afirmar que l'organització no es veu afectada per baixes de determinat personal, però el reduït nombre d'administradors de sistemes existents produeix un risc de disponibilitat tant d'aquest rol com del responsable de seguretat.

7. PROPOSTES DE PROJECTES

7.1 INTRODUCCIÓ

En aquest punt s'enumeraran diferents projectes per tal de millorar el nivell de compliment de la ISO pels diferents dominis, així com per mitigar el risc al que estan exposats certs actius. Per tant, s'empraran els nivells de compliment dels diferents dominis de la ISO 27001 i l'anàlisi de riscos realitzats en els apartats anteriors, els quals ens aporten un coneixement exacte de l'estat actual de la seguretat, per tal de poder plantejar i definir quin tipus de projectes, iniciatives o millores són més necessàries o urgents per tal de millorar la seguretat de l'organització.

Els projectes seleccionats poden aportar a l'organització una major optimització dels recursos, millores en la gestió de processos i tecnologies emprades en l'organització. Un punt important a tenir en compte és que no cal que siguin dins l'àmbit de la tecnologia, ja que poden afectar diferents departaments o àmbits, com per exemple recursos humans.

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

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

Per cada projecte plantejat s'inclourà un punt on s'indicarà com afecta el projecte al compliment o a l'anàlisi de riscos, mentre que al final de l'apartat, en el punt 7.5, es mostraran les conclusions així com l'impacte dels projectes en el seu conjunt a l'estat actual de l'organització.

Els diferents impactes positius per l'organització juntament amb la valoració econòmica de les diferents opcions ajudarà al Govern Municipal a decidir quines actuacions convé realitzar, i per tant en quines és necessari invertir diners.

7.2 PROJECTES A CURT TERMINI

A continuació es presenten un conjunt de projectes a implantar durant el primer any del període, establert en tres anys:

- **PROJ-001:** Adquisició de programari antivirus corporatiu
- **PROJ-002:** Procediments d'actualitzacions de sistemes operatius
- **PROJ-003:** Documentació / Implantació de Polítiques de Seguretat
- **PROJ-004:** Realització de l'inventari d'actius
- **PROJ-005:** Millora de climatització en els Centre de Processament de Dades
- **PROJ-006:** Revisió de procediments en Recursos Humans

7.2.1 ADQUISICIÓ DE PROGRAMARI ANTIVIRUS CORPORATIU

Tal i com es pot observar en l'anàlisi de riscos (apartat 6.6), es detecta un risc molt elevat a la major part dels sistemes operatius de l'organització. Actualment s'utilitza un programari d'antivirus antic, el qual no permet la seva instal·lació en servidors i genera problemes en certes estacions de treball. Com que es tracta d'un punt de l'anàlisi de riscos que s'ha considerat bastant crític i no comporta una despesa molt elevada, es proposa l'execució d'aquest projecte el més aviat possible, per tant, es realitzaria durant el primer any.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-001**
NOM:	**ADQUISICIÓ DE PROGRAMARI ANTIVIRUS CORPORATIU**
OBJECTIUS:	- Control de virus i altre tipus de programari maliciós en clients. - Implantació d'antivirus en servidors Windows. - Reducció de tràfic de xarxa i consum Internet
ABAST:	- Estacions de treball Windows XP SP3 o superiors (Software). - Servidors Windows 2003 o superiors (Software).
DESCRIPCIÓ:	- Instal·lació de versió corporativa de programari antivirus, ja que actualment no existeix i se'n detecta una carència clara. - Definició d'actualitzacions dels clients periòdiques i automatitzades, si pot ser en un servidor local centralitzat per no saturar la connexió a Internet.
ACTIVITATS:	- Selecció d'empresa proveïdora segons capacitats i

	requeriments (sistemes operatius, cost llicències, rendiment d'estacions de treball i servidors amb servei antivirus habilitat). - Configuració del desplegament. - Instal·lació de proves en servidor i estacions de treball. - Desplegament a la resta de servidors i estacions de treball. - Actualitzacions periòdiques automàtiques. - Consulta estadístiques de detecció globals (control ISO).
BENEFICIS:	- Eliminació o bloqueig de programari maliciós en tots els sistemes. - Reducció del tràfic de xarxa. - Centralització de la gestió. - Facilitat d'implementació de controls ISO (mitjançant estadístiques globals de detecció).
COST ECONÒMIC:	**2.500 €** (llicències suficients per servidors i estacions de treball).
TEMPS EXECUCIÓ:	**2 mesos** entre selecció, compra, proves, instal·lació en equips i configuració.
AFECTACIÓ AARR:	Redueix considerablement el risc en l'àmbit dels Sistemes Operatius, que tenien un risc màxim en confidencialitat, integritat i disponibilitat.
AFECTACIÓ ISO:	**10.4 – Protecció contra codi maliciós:** passaria a nivell L5.

Taula 7-1: Projecte PROJ-001

Tal i com s'esmenta en la *Taula 7-1*, la implementació del projecte PROJ-001 permetria reduir el risc dels sistemes operatius. Mitjançant aquest projecte es redueix molt considerablement el risc, ja que la probabilitat de risc es reflectia elevada en els sistemes operatius degut a la presència freqüent de codi maliciós.

En canvi, el compliment de la ISO es veu afectat però no massa, ja que ja existia control previ al codi maliciós i estava comptabilitzat. Tot i així, incrementa 0,2 punts el percentatge de compliment del domini 10 de la ISO: Gestió de comunicacions i operacions. Per tant, l'augment del compliment de la ISO 27001 en els diferents dominis no es veu pràcticament afectat, tal i com es mostra en la *Figura 7-1*.

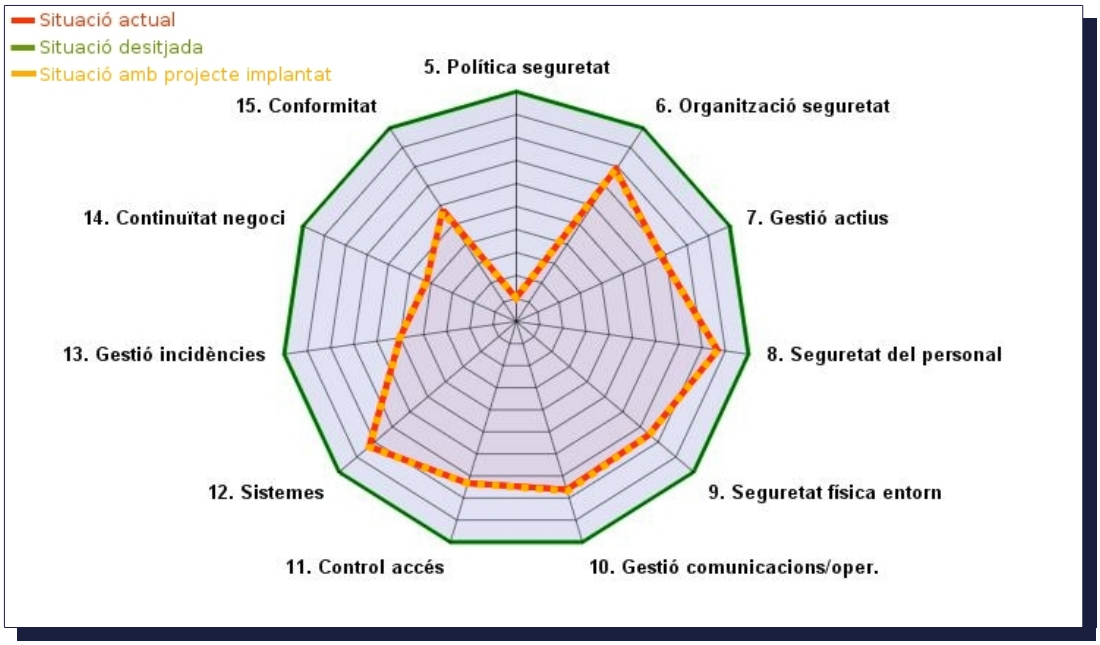

Figura 7-1: Diagrama de radar del compliment ISO després d'implantar PROJ-001

7.2.2 PROCEDIMENTS D'ACTUALITZACIONS EN SISTEMES OPERATIUS

Aquest projecte consisteix en l'establiment d'uns procediments per tal de realitzar adequadament les actualitzacions dels sistemes operatius.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	PROJ-002
NOM:	PROCEDIMENTS D'ACTUALITZACIONS EN SISTEMES OPERATIUS
OBJECTIUS:	- Descarregar i aplicar actualitzacions de seguretat en sistemes operatius de servidors Windows i Linux. - Mantenir actualitzades les diferents estacions de treball. - Reduir impacte de possibles virus.
ABAST:	- Estacions de treball Windows XP SP3 o superiors (Software). - Servidors Windows 2003 o superiors (Software). - Servidors Linux Debian/Ubuntu Server.
DESCRIPCIÓ:	- Cal descriure un procediment d'actualització d'estacions de treball (pot ser automàtic degut a que es reinicien sovint). - Cal descriure un procediment per executar les actualitzacions de seguretat dels sistemes operatius. En aquest

	cas cal preveure un reinici periòdic del servidor per tal d'aplicar els canvis.
ACTIVITATS:	- Definició de nou procediment per actualitzacions d'estacions de treball. - Definició de nou procediment per actualitzacions de seguretat de servidors Windows. - Definició de nou procediment per actualitzacions de seguretat de servidors Windows. - Implementació de control: reinici efectuats dels servidors / reinicis programats del servidor durant un període de temps. En cas d'estacions de treball, el control pot ser el percentatge d'estacions de treball amb actualitzacions pendents o deshabilitades dins un període determinat de temps.
BENEFICIS:	- Reducció de vulnerabilitats en els diferents sistemes. - Reducció de l'impacte en possibles infeccions.
COST ECONÒMIC:	**0 €**. Implementació interna.
TEMPS EXECUCIÓ:	**1 mes** sense dedicació a temps complet.
AFECTACIÓ AARR:	Redueix considerablement el risc en l'àmbit dels Sistemes Operatius, que tenien un risc màxim en confidencialitat, integritat i disponibilitat.
AFECTACIÓ ISO:	**10.4 – Protecció contra codi maliciós:** passaria a nivell L5. **9.2.4 – Manteniment dels equips:** de nivell L3 a nivell L5.

Taula 7-2: Projecte PROJ-002

Juntament amb el **PROJ-001** (adquisició de programari antivirus), uns bons procediments d'actualització dels sistemes operatius permet seguir reduint el possible risc dels sistemes operatius. De totes maneres, el diagrama de radar (*Figura 7-2*) no canvia substancialment del de la *Figura 7-1*, ja que afecta poc els dominis 9 i 10 de la ISO.

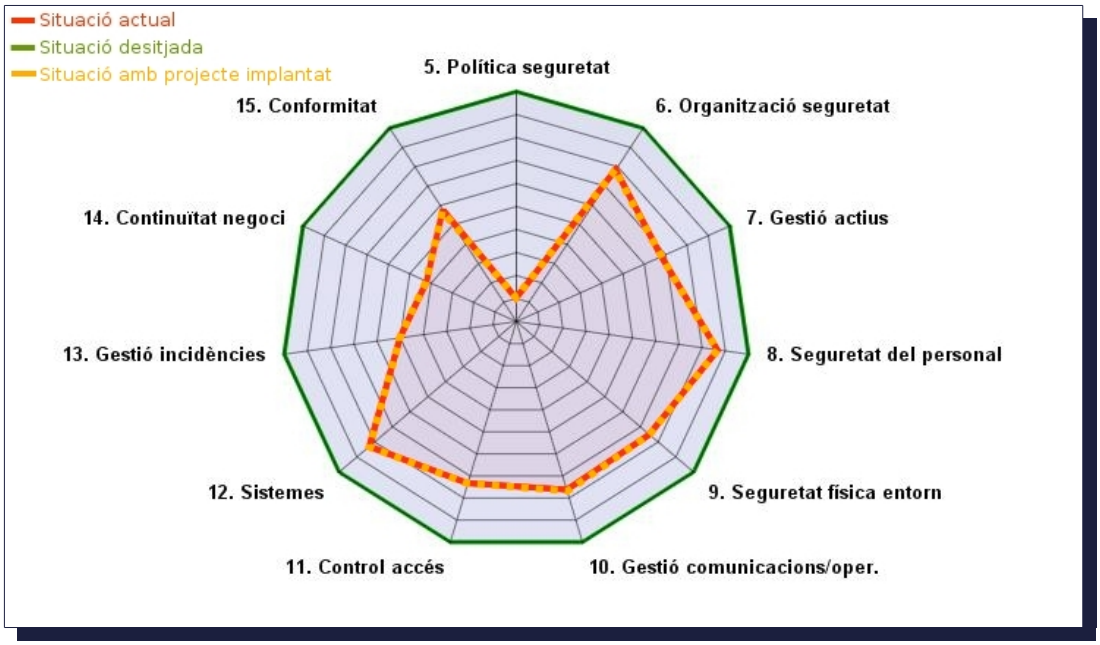

Figura 7-2: Diagrama de radar del compliment ISO després d'implantar PROJ-002

7.2.3 DOCUMENTACIÓ/IMPLANTACIÓ DE POLÍTIQUES DE SEGURETAT

Tal i com es mostra en la *Figura 4-2*, l'organització no contempla gairebé cap control en el domini de la Política de Seguretat dins el marc de la ISO 27001. Per tant, mitjançant aquest projecte es desitja aprovar i implementar la Política de Seguretat així com la resta de procediments esmentats en l'actual document que hi estiguin relacionats. És un pas necessari per tal que els diferents rols relacionats amb la seguretat puguin exercir les funcions que els hi corresponen. Sense política, aquests rols definits no tenen cap tipus de sentit.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-003**
NOM:	**DOCUMENTACIÓ/IMPLANTACIÓ DE POLÍTIQUES SEGURETAT**
OBJECTIUS:	- Definició, aprovació i aplicació de les Polítiques de Seguretat necessàries.
ABAST:	- Departaments de l'organització. - Direcció (Govern Municipal o Junta de Govern Local).
DESCRIPCIÓ:	- Definició de Política de seguretat de l'organització (partint del model presentat en el present document).

	- Definició de: normes de seguretat, procediments de seguretat, procediments operatius de seguretat i instruccions tècniques. - Aprovació i implantació en l'organització un cop aprovada. - Revisió dos cops l'any de la Política de Seguretat.
ACTIVITATS:	- Definició de Política de seguretat. - Proposta de Polítiques a Junta de Govern Local - Modificació segons propostes de JGL. - Aprovació de Política de Seguretat per part de la JGL. - Implantació de la Política de Seguretat. - Informar-ne degudament als empleats, per tal que la coneguin i en disposin en diferents formats (paper/electrònic). - Implementació de control: percentatge de revisions periòdiques realitzades respecte les previstes.
BENEFICIS:	- Definició ferma dels diferents rols. - Fer palès que la direcció es preocupa i desitja millorar la seguretat de l'organització en l'àmbit de les tecnologies de la informació i la comunicació. - Informar a tots els treballadors de les polítiques de seguretat definides i aprovades per la direcció. - Documentació necessària per l'Esquema Nacional de Seguretat (ENS).
COST ECONÒMIC:	**5.500 €**. Despeses en dietes per comissions/hores extraordinàries i posar en disposició dels empleats els documents necessaris en format electrònic/paper.
TEMPS EXECUCIÓ:	**10 mesos**
AFECTACIÓ AARR:	Cap directament.
AFECTACIÓ ISO:	**- 5.1.1 Document de política de seguretat:** degut a que no està totalment implantada, passaria de L0 a L4. En posteriors revisions podríem considerar-la L5. **- 5.1.2 Revisions de la política de seguretat: P**assaria de L0 a L3. En posteriors revisions podríem considerar-la L4 o L5 si es compleixen les revisions periòdiques.

Taula 7-3: Projecte PROJ-003

Amb la execució i implantació del **PROJ-003**, l'organització ja disposarà d'una Política de Seguretat que caldrà aplicar en tot moment i per tots els seus treballadors. Es realitza en aquesta primera fase degut a que és un pas totalment necessari per l'aplicació de certs procediments i projectes addicionals.

En la *Figura 7-3* es pot apreciar com el valor de compliment de la ISO 27001 pel domini 5 ('Política de seguretat') augmenta considerablement respecte la situació actual.

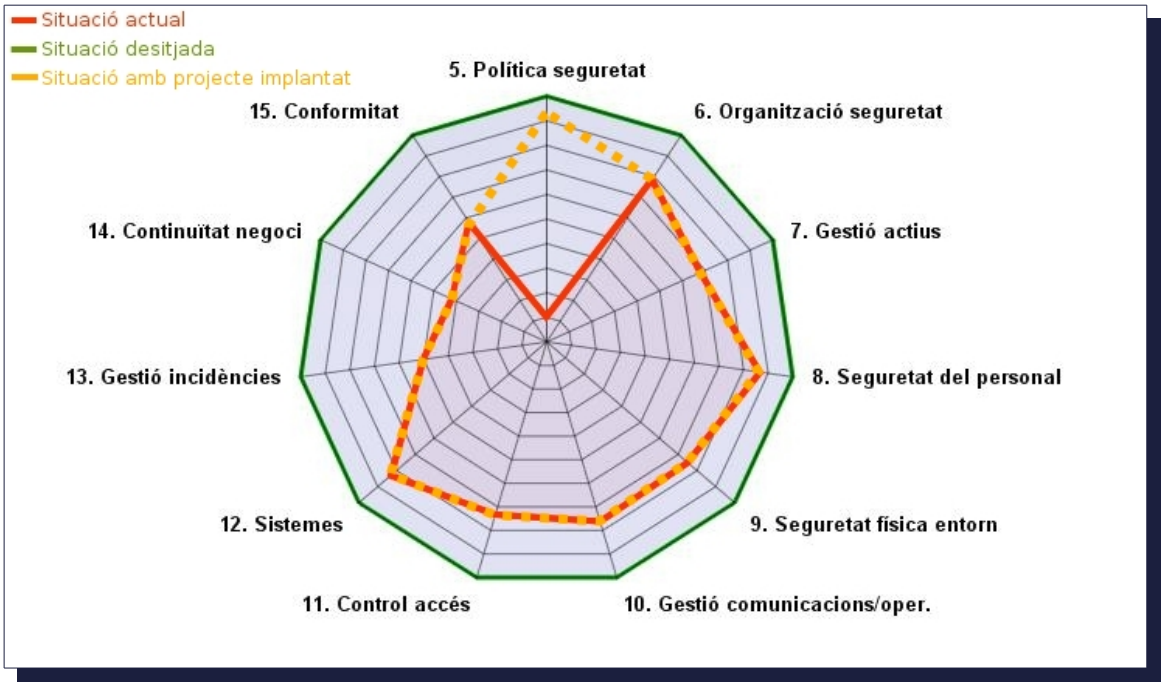

Figura 7-3: Diagrama de radar 'compliment ISO' després d'implantació del PROJ-003

7.2.4 REALITZACIÓ DE L'INVENTARI D'ACTIUS

Actualment l'organització no disposa de cap inventari d'actius actualitzat. Per tant, mitjançant l'execució del present projecte es desitja disposar d'un inventari exhaustiu i amb possibilitat de gestió i manteniment posterior.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-004**
NOM:	**REALITZACIÓ DE L'INVENTARI D'ACTIUS**
OBJECTIUS:	- Realització de l'inventari d'actius dels diferents departaments

	de l'organització.
ABAST:	- Actius de l'organització relacionats amb les tecnologies de la informació i la comunicació.
DESCRIPCIÓ:	- Creació d'un fitxer (fulla càlcul o base de dades i programari) per tal d'inventariar els diferents actius relacionats amb les tecnologies de la informació i comunicació.
ACTIVITATS:	- Definició de base de dades i documentació a gestionar per cada actiu. - Elaboració d'inventari d'actius exhaustiu. - Gestió i manteniment dels actius. - Implementació de control: elements no inventariats detectats cada any.
BENEFICIS:	- Control dels diferents actius. - Explotació de les dades per altres fins (finalitzacions de garanties o manteniments, elements antics, etc.). - Facilita la definició d'actius de l'Anàlisi de riscos.
COST ECONÒMIC:	**500 €**. Ús de personal intern i estudiant en pràctiques.
TEMPS EXECUCIÓ:	**2 mesos**
AFECTACIÓ AARR:	Cap directament, però pot ajudar en el manteniment el fet de disposar d'aquest inventari.
AFECTACIÓ ISO:	**- 7.1.1 Inventari d'actius:** L'organització passaria del nivell L2 actual al L5.

Taula 7-4: Projecte PROJ-004

Amb la execució i implantació del **PROJ-004**, l'organització disposarà d'un inventari exhaustiu dels diferents actius. La *Figura 7-4* mostra el canvi que comportaria en el compliment de la norma ISO 27001:

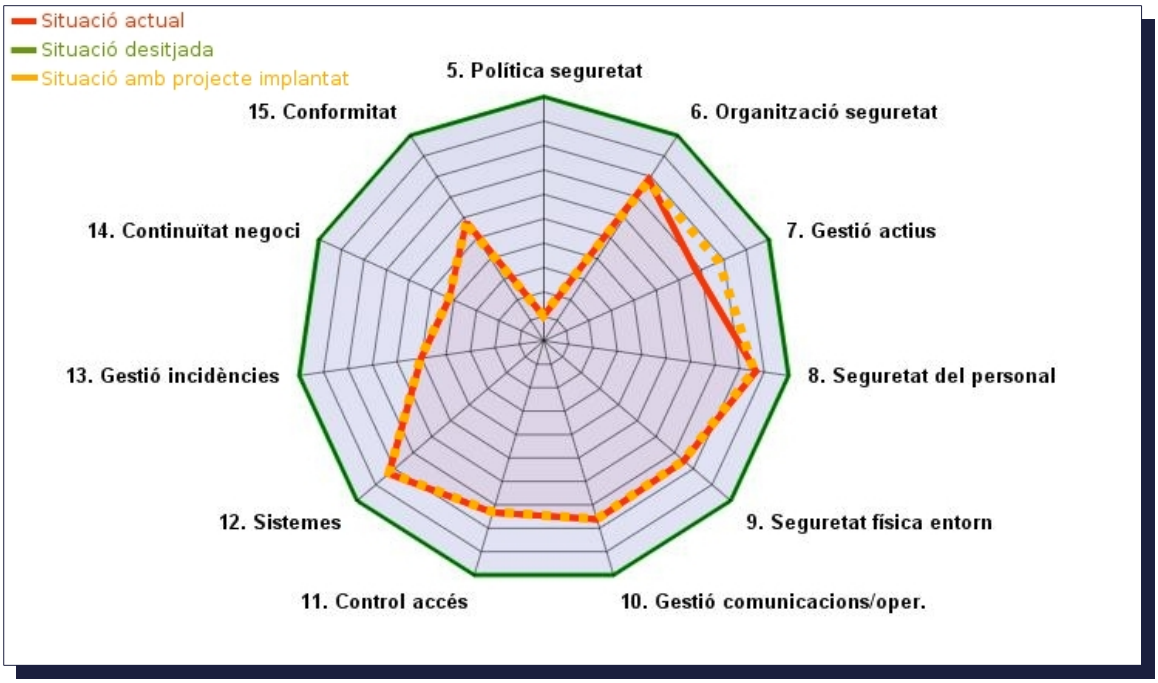

Figura 7-4: Diagrama de radar 'compliment ISO' després d'implantació del PROJ-PROC-004

7.2.5 MILLORA DE CLIMATITZACIÓ EN ELS CENTRES DE PROCESSAMENT DE DADES

Actualment l'organització no disposa de cap inventari d'actius actualitzat. Per tant, mitjançant l'execució del present projecte es desitja disposar d'un inventari exhaustiu i amb possibilitat de gestió i manteniment posterior.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-005**
NOM:	**MILLORA DE CLIMATITZACIÓ EN ELS CPD**
OBJECTIUS:	- Millora de la climatització dels diferents Centres de Processament de Dades que posseeix actualment l'Ajuntament (actualment es mostren insuficients).
ABAST:	- Els 4 centres de processament de dades.
DESCRIPCIÓ:	- Actualment dels quatre CPD existents, només un refrigera correctament pels elements existents, tot i que ja no permetria afegir més elements generadors de calor. Dels altres tres, dos tenen problemes durant els mesos d'estiu, mentre que el restant disposa d'un aparell de climatització antic que

	sovint no funciona correctament.
ACTIVITATS:	- Dimensionament de la refrigeració segons dimensió de sales i elements irradiants d'energia calorífica. - Cerca de proveïdor i compra d'elements necessaris. - Instal·lació d'equipament. - Instal·lació de sensors de temperatura que es comuniquin amb Nagios o gestor d'alertes. - Implementació de control: Percentatge de dies amb alertes dels sensors. - Definició de períodes de revisió dels aparells per personal especialitzat (contracte anual) o personal de la casa (oficina tècnica - lampisteria).
BENEFICIS:	- Maquinari treballant en condicions idònies de temperatura. - Explotació de les dades per altres fins (finalitzacions de garanties o manteniments, elements antics, etc.). - Facilita la definició d'actius de l'Anàlisi de riscos.
COST ECONÒMIC:	**12.000 €**. (3.000 € per cada CPD).
TEMPS EXECUCIÓ:	**4 mesos**
AFECTACIÓ AARR:	En bona part dels actius de Hardware o maquinari que resideixen en els CPD s'observa que l'amenaça més important que pateixen és la de condicions inadequades de temperatura. Això és degut a la mala climatització en la major part dels CPD. Amb aquest projecte es solucionaria aquest tipus d'amenaça, la qual afecta segons l'Anàlisi de Riscos a elements els quals tenen un gran impacte sobre l'organització ([HW.1], [HW.2], [HW.11], [HW.12], [HW.18], [HW.20], etc.).
AFECTACIÓ ISO:	**- 9.1.4 Protecció enfront amenaces externes i d'entorn:** L'organització passaria del nivell L2 actual a L3. Protegiria davant amenaces d'entorn, no afectaria a les d'entorn. **- 9.2.4 Manteniment dels equips:** Redueix la possibilitat de problemes amb components electrònics degut a altes temperatures. En aquest cas passaria d'estar en un nivell L3 a L4.

Taula 7-5: Projecte PROJ-005

Amb la execució i implantació del **PROJ-005**, l'organització eliminarà bona part dels riscos de maquinari que s'observen en la *Figura 6-3* i *Taula 6-11* de l'anterior apartat. Analitzant els riscos de disponibilitat que presenten aquests actius, pràcticament tots venen donats per funcionament sota temperatura inadequada.

La *Figura 7-5* mostra el canvi que comportaria en el compliment de la norma ISO 27001, en el domini 9 (Seguretat física i de l'entorn):

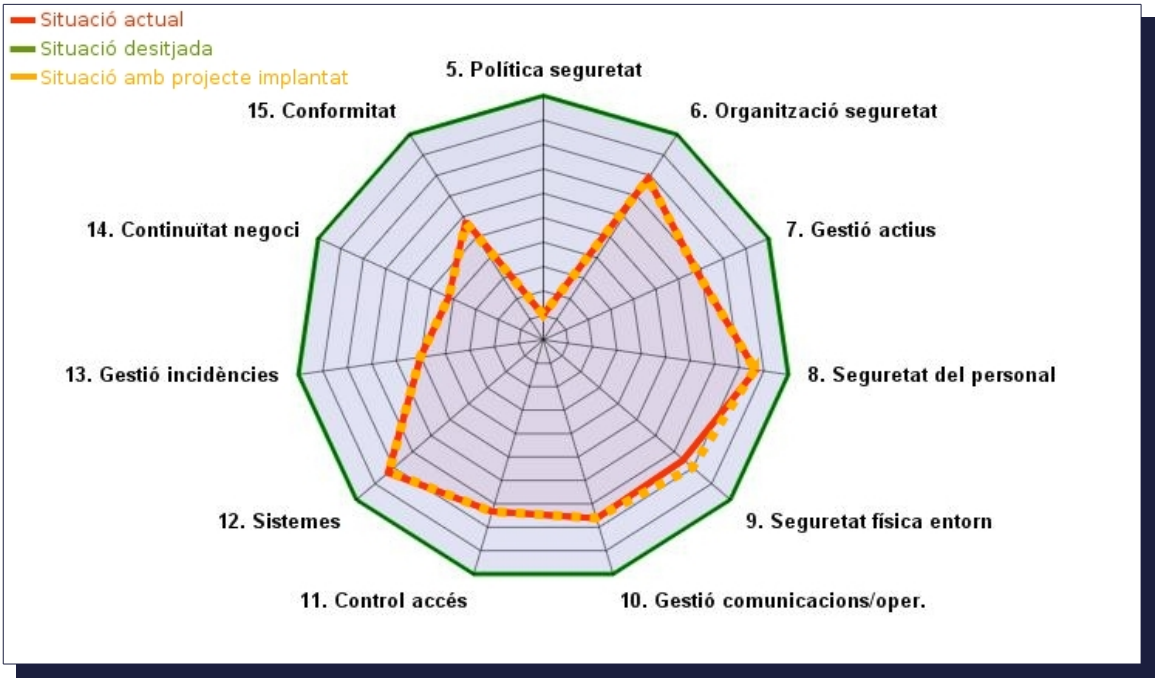

Figura 7-5: Diagrama radar del compliment ISO amb el PROJ-PROC-005

7.2.6 REVISIÓ DE PROCEDIMENTS EN RECURSOS HUMANS

L'anàlisi de riscos realitzat mostra una freqüència alta d'errors d'usuari que suposa un compromís per les dades relacionades amb els recursos humans de l'organització. Degut a la importància i sensibilitat d'aquestes dades, l'organització necessita reduir el risc d'aquest tipus d'actiu per evitar problemes amb la seva integritat i confidencialitat. Per tant, es defineix el següent projecte **PROJ-006** per tal de revisar els diferents procediments existents dins del departament de recursos humans per tal de depurar-los i adaptar-los a la nova política de seguretat, definida en el **PROJ-003**.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-006**
NOM:	**REVISIÓ DE PROCEDIMENTS DE RECURSOS HUMANS**

OBJECTIUS:	- Millores en els procediments del departament de Recursos Humans per tal de fer-los més segurs i confidencials.
ABAST:	- Departament de Recursos Humans.
DESCRIPCIÓ:	- L'anàlisi de riscos indica que alguns procediments del departament de Recursos Humans, ja sigui per falta d'indicacions a l'usuari o per error humà, presenten un elevat risc en la confidencialitat i integritat de les dades. Això pot provocar el coneixement de dades sensibles per part de tercers. Cal revisar els procediments per tal de fer-los més segurs i que el personal del departament actuï de manera correcta per evitar aquest tipus d'incidències.
ACTIVITATS:	- Revisió de les impressions protegides per nòmines i altres informacions. - Accés al despatx quan no hi hagi personal del departament present. - Comunicació d'altes i baixes a certs departaments que precisen tenir-ne coneixement.
BENEFICIS:	- Confidencialitat de nòmines, baixes i altra informació sensible. - Altes i baixes d'usuaris en altres sistemes més ràpida i segura.
COST ECONÒMIC:	**500 €**. No caldria contractació externa.
TEMPS EXECUCIÓ:	**2 mesos**
AFECTACIÓ AARR:	Eliminaria l'alta probabilitat d'errades d'usuari en els processos relacionats amb l'actiu de dades de personal i nòmines [D.10].
AFECTACIÓ ISO:	**- 10.7.3 Procediments d'utilització de la informació: P**assaria del nivell L1 actual a L3.

Taula 7-6: Projecte PROJ-006

Amb l'execució de **PROJ-006**, el departament de Recursos Humans gestionarà correctament l'actiu de dades de nòmines, altes, baixes i altra informació sensible de l'organització. Això facilitarà la reducció dels errors, i per tant es reduirà el risc detectat en l'anàlisi respecte l'actiu [D.10].

La *Figura 7-6* mostra el canvi que comportaria en el compliment de la norma ISO 27001.

tot i afectar un objectiu de control del domini 10, el diagrama de radar del compliment ISO no detecta un gran canvi.

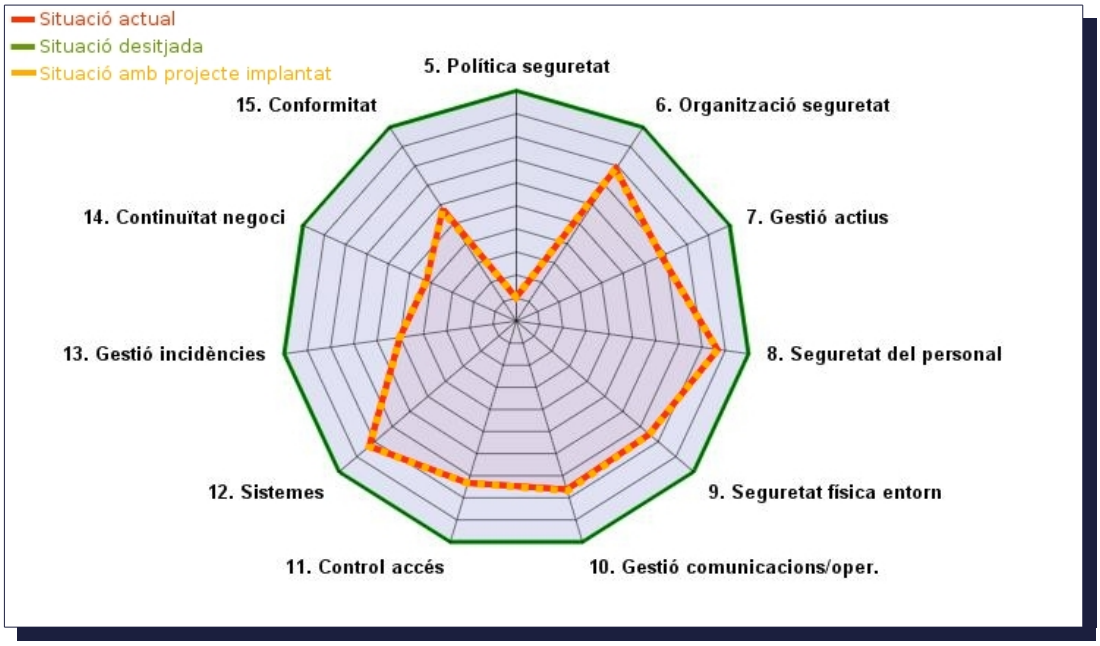

Figura 7-6: Diagrama radar del compliment ISO amb el PROJ-PROC-006

7.3 PROJECTES A MIG TERMINI

A continuació es presenten un conjunt de propostes de projectes a implantar durant el segon any del període:

- **PROJ-007:** Formació del personal en seguretat de les TIC
- **PROJ-008:** Gestió d'incidències – Programari i procediments
- **PROJ-009:** Definició de plans de continuïtat
- **PROJ-010:** Definició de procediments de còpies de seguretat

7.3.1 FORMACIÓ DEL PERSONAL EN SEGURETAT DE LES TIC

Degut a que l'anàlisi de riscos mostra certes amenaces d'erros d'usuari amb una freqüència alta, es proposa la realització de cursos de Seguretat per tots els empleats. Aquests cursos, de realització periòdica i obligatòria serviran per formar al personal respecte temes de seguretat, ja siguin genèrics o respecte eines o dispositius que utilitzin en les seves tasques diàries.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	PROJ-007
NOM:	FORMACIÓ DEL PERSONAL EN SEGURETAT DE LES TIC
OBJECTIUS:	- Reduir la freqüència d'amenaces en certs actius on apareix una freqüència alta d'errors d'usuari. - Formar tot el personal de manera periòdica per conscienciar-los respecte la seguretat de la informació i millorar els seus procediments.
ABAST:	- Tots els departaments de l'organització.
DESCRIPCIÓ:	- Es realitzaran cursos de formació a tots els empleats relatius a la Seguretat de les Tecnologies de la Informació i la Comunicació. Aquests cursos disposaran de temari genèric i temari específic segons les eines o dispositius que l'Ajuntament utilitzi.
ACTIVITATS:	- Decisió de temes o aspectes a incloure. - Cercar empresa per realitzar la formació i contractació. - Establiment definitiu del temari i planificació (anual) de les sessions de formació. - Realització de sessions. - Enquestes de satisfacció (o examen de coneixements) per implementar algun control.
BENEFICIS:	- Conscienciació en matèria de seguretat. - Reducció dels errors d'usuari deguts a desconeixement de certs aspectes de la seguretat en els TIC. - La formació addicional del personal pot suposar un valor afegit als empleats si la troben d'utilitat.
COST ECONÒMIC:	**5.000 €**. (anuals)
TEMPS EXECUCIÓ:	**4 mesos**
AFECTACIÓ AARR:	Eliminaria l'alta probabilitat d'errades d'usuari en els processos relacionats amb l'actiu de dades de personal i nòmines [D.10], així com els de correu electrònic [D.9].
AFECTACIÓ ISO:	**- 8.2.2 Conscienciació, formació i capacitació de seguretat:** Passaria del nivell L2 actual a L5.

Taula 7-7: Projecte PROJ-007

Mitjançant el PROJ-007, el compliment del domini 8 de la ISO, Seguretat del personal, passa a ser del 86,67% actual, al 92,22%. Estem realitzant una millora en un punt que ja estava bastant ben cobert, però és un projecte encarat a reduir cert tipus de riscos més que a una millora del compliment de la ISO. Tot i així, en la *Figura 7-7* es pot apreciar el canvi que comportaria en el compliment de la norma ISO 27001.

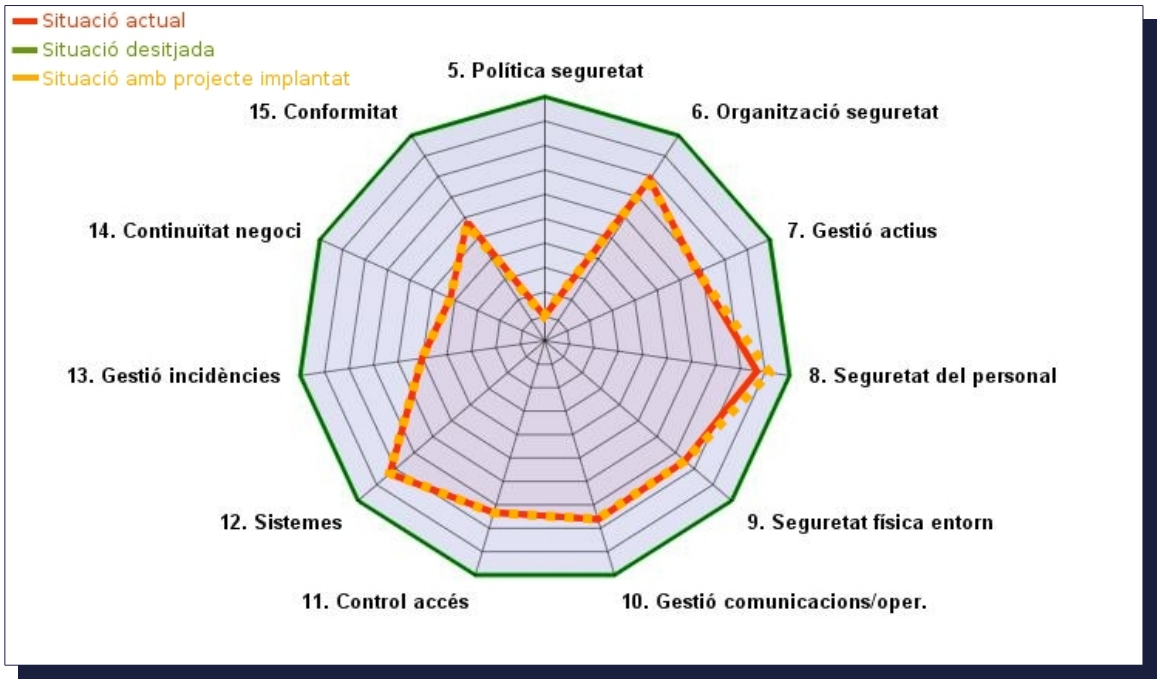

Figura 7-7: Diagrama radar del compliment ISO amb el PROJ-PROC-007

7.3.2 GESTIÓ D'INCIDÈNCIES: PROGRAMARI I PROCEDIMENTS

Interpretant el compliment actual de la ISO, està clar actualment l'Ajuntament de Riberola no disposa d'una gestió d'incidències apropiada. El projecte actual vol pal·liar aquesta situació mitjançant dos actuacions principals:

- Definició i implantació de procediments en la gestió d'incidències.
- Desenvolupament de programari de gestió d'incidències i documentació de les gestions realitzades.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-008**
NOM:	**GESTIÓ D'INCIDÈNCIES: PROGRAMARI I PROCEDIMENTS**
OBJECTIUS:	- Definir procediments clars, rols i responsabilitats en la gestió

	de les incidències TIC que puguin aparèixer. - Utilització de programari per facilitar la gestió d'aquestes incidències, així com permetre documentar la resolució de les diferents incidències per consulta posterior o extreure estadístiques.
ABAST:	- Departament TIC, altres departaments per poder fer l'alta de les incidències.
DESCRIPCIÓ:	- Es definiran procediments, rols i responsabilitats en la gestió de les incidències. - Es desenvoluparà un programari capaç de rebre les incidències relacionades amb les tecnologies de la informació i la comunicació dels diferents departaments de l'Ajuntament. A més, permetrà al departament TIC gestionar les diferents incidències, anotar la seva resolució (per consultes posteriors) i la generació d'estadístiques per detectar possibles problemes que es repeteixen en el temps o en certs departaments.
ACTIVITATS:	- Definició de procediments, rols i responsabilitats. - Desenvolupament del programari o adaptació d'existent. - Període de proves del programari (2 o 3 departaments amb accés per introduir incidències). - Habilitació de la resta de departaments. - Extracció d'estadístiques (incidències gestionades, solucionades, departament que més en genera, incidències més repetides, etc.). - Addicionalment, integració d'alertes Nagios i IDS.
BENEFICIS:	- Conscienciació en matèria de seguretat. - Reducció dels errors d'usuari deguts a desconeixement de certs aspectes de la seguretat en els TIC. - La formació addicional del personal pot suposar un valor afegit als empleats si la troben d'utilitat. - Integració de totes les incidències en un sol lloc.
COST ECONÒMIC:	**12.700 €**. Desenvolupament del programari.
TEMPS EXECUCIÓ:	**8 mesos**

AFECTACIÓ AARR:	Una bona gestió de les incidències pot aportar una reducció d'amenaces en certs actius, ja que ajudarà a detectar problemes reiteratius en diferents departaments de l'organització.
AFECTACIÓ ISO:	**- 13 Gestió d'incidències:** Afectaria diferents objectius de control, millorant de manera considerable el seu compliment.

Taula 7-8: Projecte PROJ-008

En la *Figura 7-8* es pot apreciar el canvi que comportaria en el compliment de la norma ISO 27001.

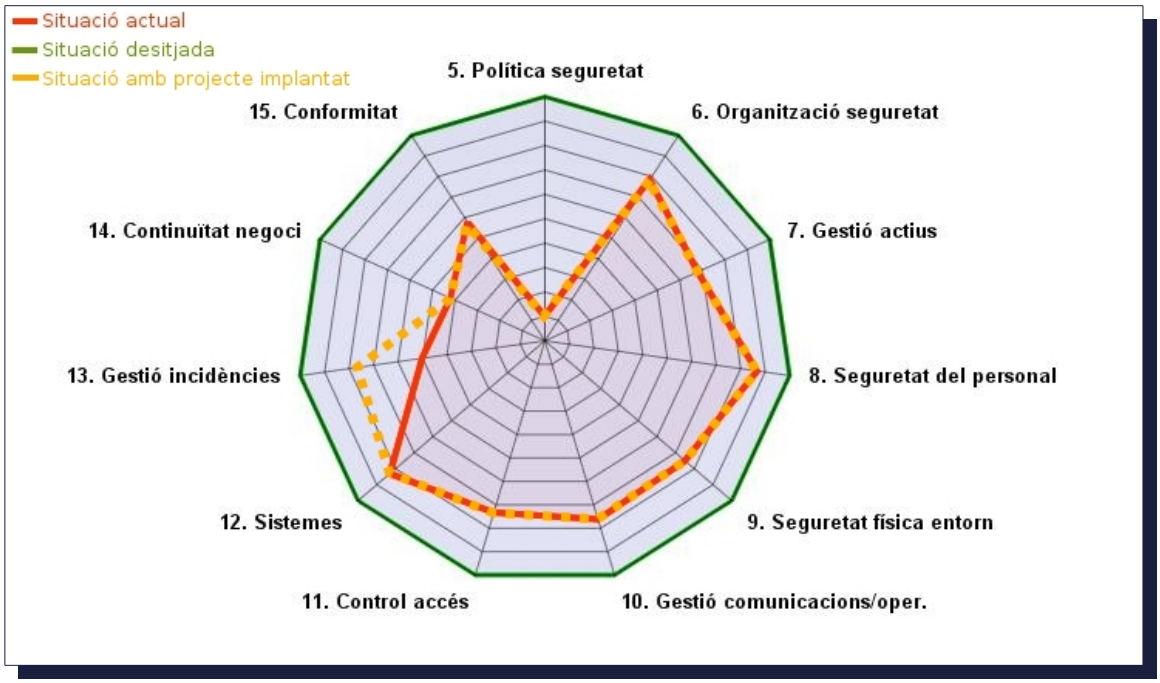

Figura 7-8: Diagrama radar del compliment ISO amb el PROJ-PROC-008

7.3.3 DEFINICIÓ DE PLANS DE CONTINUÏTAT

Actualment l'Ajuntament no disposa de plans de continuïtat degudament documentats o especificats. Per tant, en cas de necessitat, poden succeir dubtes o mal entesos en l'execució dels diferents procediments necessaris per permetre la continuïtat de l'activitat normal de l'organització.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-009**
NOM:	**DEFINICIÓ DE PLANS DE CONTINUÏTAT**

OBJECTIUS:	- Documentar els diferents procediments per, en cas d'emergències o materialització d'unes amenaces en concret, permetre al continuïtat de l'activitat de l'Ajuntament en uns serveis mínims definits (i aprovats).
ABAST:	- Departament TIC, departaments amb atenció al ciutadà i policia municipal (emergències).
DESCRIPCIÓ:	- Es definiran diferents plans de continuïtat en diferents aspectes, sempre relacionats amb elements de les tecnologies de la informació i la comunicació o serveis relacionats.
ACTIVITATS:	- Determinació dels diferents plans. - Per cada pla, acordar els serveis mínims (per part de direcció o JGL). - Documentació dels diferents procediments per cada pla. - Execució de projectes necessaris per aplicar els plans (si s'escau). - Realització periòdica de proves dels plans, sempre que no afecti la continuïtat de l'activitat normal (fora hores).
BENEFICIS:	- Assegurar la prestació de serveis als ciutadans en cas de patir cert tipus d'emergències o problemes, mitjançant uns serveis mínims. - Proporcionar al personal una documentació amb la qual reduir dubtes i marcar els procediments específics per iniciar el pla de continuïtat corresponent en cas de necessitat.
COST ECONÒMIC:	**10.000 €**. Material, contractacions, projectes, etc.
TEMPS EXECUCIÓ:	**10 mesos**
AFECTACIÓ AARR:	Podria reduir el risc de molts dels actius, sobretot en la dimensió de la disponibilitat, ja que proporciona els elements necessaris per a que certs actius segueixin estant disponibles tot i patir la materialització d'alguna amenaça concreta.
AFECTACIÓ ISO:	**- 14 Continuïtat del negoci:** Afectaria diferents objectius de control, millorant-ne molt el seu compliment per part de l'organització.

Taula 7-9: Projecte PROJ-009

Mitjançant el **PROJ-009**, el compliment del domini 14 de la ISO, Continuïtat del negoci, passa a ser del 86,67% actual, al 92,22%. En el següent anàlisi de riscos un cop executat el projecte, es reduirà el risc en el domini de la disponibilitat en certs actius. En la *Figura 7-9* es pot apreciar el canvi que comportaria en el compliment de la norma ISO 27001.

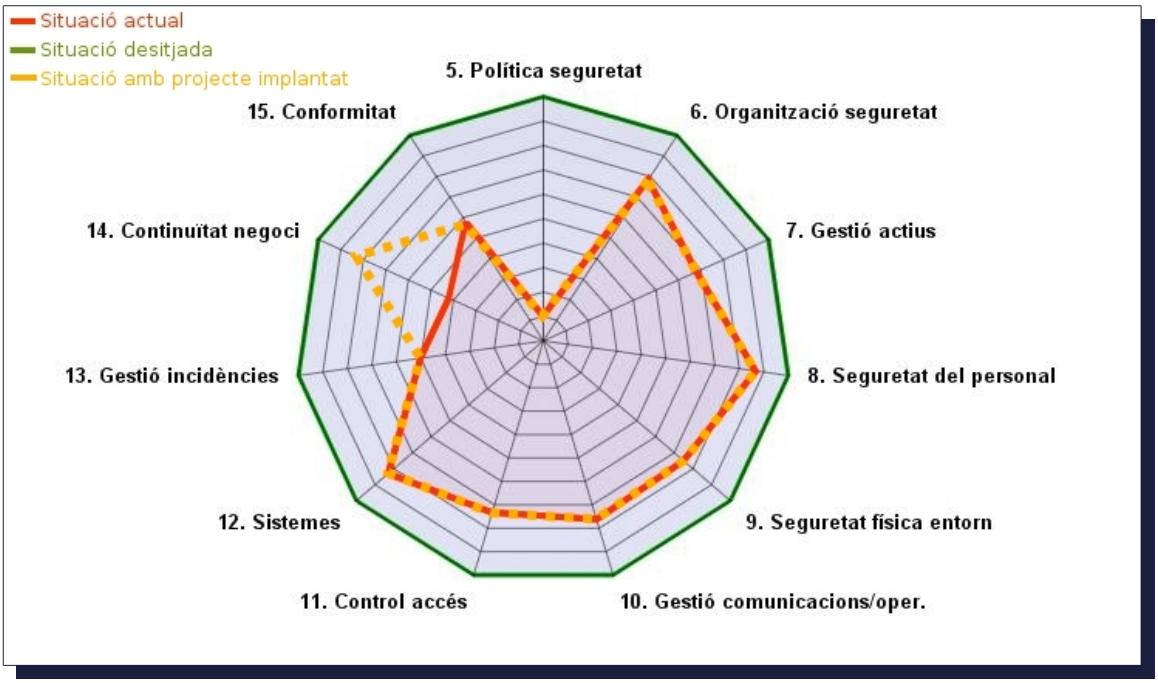

Figura 7-9: Diagrama radar del compliment ISO amb el PROJ-PROC-009

7.3.4 DEFINICIÓ DE PROCEDIMENTS DE CÒPIES DE SEGURETAT

Fent un cop d'ull a la llista d'actius amb més risc, apareix també l'actiu que fa referència a les còpies de seguretat [D.20]. Si analitzem la informació, la disponibilitat d'aquest actius es veu greument afectada per l'alta freqüència de l'amenaça d'errors de monitorització. Degut a la importància estratègica de l'actiu per l'organització, es presenta aquest projecte per tal de reduir considerablement aquesta amenaça.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-010**
NOM:	**DEFINICIÓ DE PROCEDIMENTS DE CÒPIES DE SEGURETAT**
OBJECTIUS:	- Definir i documentar formalment tots els procediments per a realitzar les còpies de seguretat de l'organització.
ABAST:	- Departament TIC.
DESCRIPCIÓ:	- Cal definir i documentar els procediments per dur a terme la realització de les còpies de seguretat. Entre aquests

	procediments hi han, entre altres, la planificació de les còpies, la gestió dels dispositius on s'emmagatzemen, les restauracions periòdiques de prova, etc.
ACTIVITATS:	- Definir i documentar la planificació de les còpies. - Definir el model de gestió dels dispositius on s'emmagatzemen les còpies de seguretat. - Definir període d'execució de proves de restauració. - Definir el procediment de monitorització de les còpies. - Revisió periòdica dels diferents procediments. - Control ISO: Restauracions correctes respecte el total
BENEFICIS:	- Assegurar la màxima disponibilitat de les còpies de seguretat.
COST ECONÒMIC:	**1.500 €.**
TEMPS EXECUCIÓ:	**2 mesos**
AFECTACIÓ AARR:	Reduiríem considerablement el risc per l'actiu [D.20] – Dades de còpies de seguretat, ja que el risc a la disponibilitat d'aquest actiu no es veuria afectat al caure la freqüència de l'amenaça dels errors de monitorització.
AFECTACIÓ ISO:	**10.5.1 RECUPERACIÓ DE LA INFORMACIÓ -** No canvia de nivell, donat que ja estava optimitzat (L5).

Taula 7-10: Projecte PROJ-010

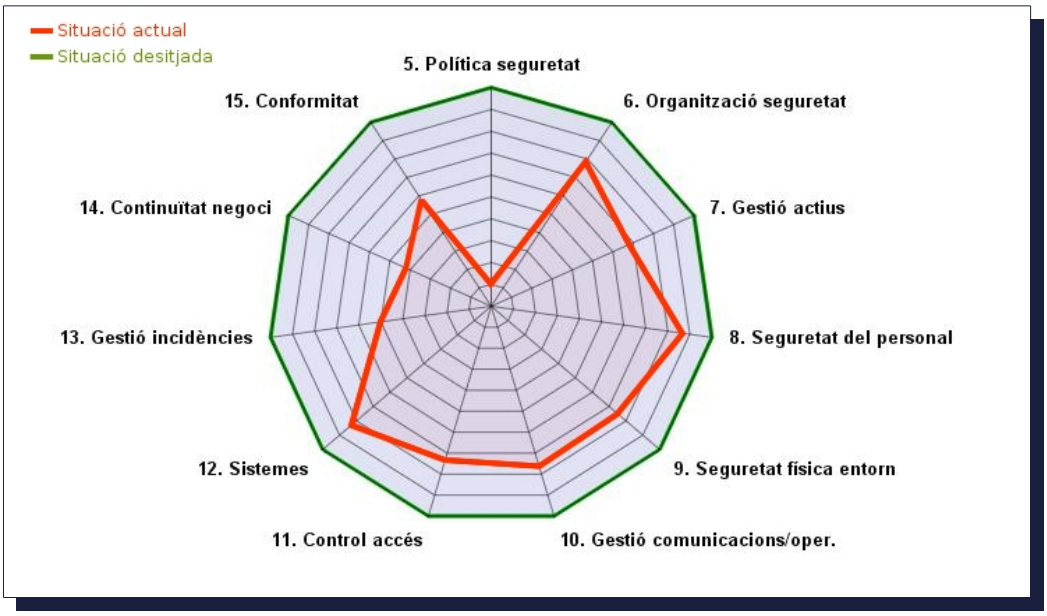

Figura 7-10: Diagrama radar del compliment ISO amb el PROJ-PROC-010

En aquest cas el canvi no comportaria cap modificació en el compliment de la norma ISO 27001 (Figura 7-10).

7.4 PROJECTES A LLARG TERMINI

A continuació es presenten un conjunt de projectes a implantar durant el tercer i últim any del període definit inicialment:

- **PROJ-011:** Procediments i gestió d'auditories internes / externes
- **PROJ-012:** Revisió i millora de polítiques d'*Active Directory* (Domini)
- **PROJ-013:** Reestructuració del departament TIC

7.4.1 PROCEDIMENTS I GESTIÓ D'AUDITORIES INTERNES / EXTERNES

Actualment no existeix cap procediment ni cap tipus de gestió respecte les auditories, ja siguin internes o externes, que cal anar realitzant periòdicament del sistema de gestió de seguretat de la informació.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-011**
NOM:	**PROCEDIMENT I GESTIÓ D'AUDITORIES INTERNES/EXTERNES**
OBJECTIUS:	- Definir, planificar, gestionar i executar auditories internes o externes de manera periòdica.
ABAST:	- Tecnologies de la Informació i la Comunicació de tota l'organització.
DESCRIPCIÓ:	- Cal definir els diferents procediments i la posterior gestió de les diferents auditories internes/externes així com els seus resultats. Per tant, mitjançant aquest projecte es definiran els procediments per fer el seguiment periòdic tant de les auditories com dels seus resultats.
ACTIVITATS:	- Definició i planificació de les diferents auditories a realitzar. - Gestionar l'execució i els resultats de les auditories. - Organitzar el tractament de les no conformitats i controlar-ne la seva correcta solució.
BENEFICIS:	- Millora del control, planificació i gestió de les diferents

	auditories i dels seus resultats.
COST ECONÒMIC:	**25.000 €.**
TEMPS EXECUCIÓ:	**5 mesos**
AFECTACIÓ AARR:	- N/A.
AFECTACIÓ ISO:	**- Diversos objectius de control del domini 15, referents a auditories**. Planificant auditories es revisaran les normes i polítiques, per tant els punts 15.2.1 (compliment de polítiques i normes) i 15.2.2 (comprovació de la conformitat tècnica) quedaran coberts amb un nivell L4. A més, el 15.3.1 (controls d'auditoria de sistemes) passarà també a nivell L4 de compliment.

Taula 7-11: Projecte PROJ-011

Mitjançant aquest projecte, es produeix una millora considerable del compliment del domini 15 de la ISO, passant d'un percentatge de compliment del 57'50% al 86%. Aquesta millora es pot observar de manera gràfica en el diagrama de la *Figura 7-11*.

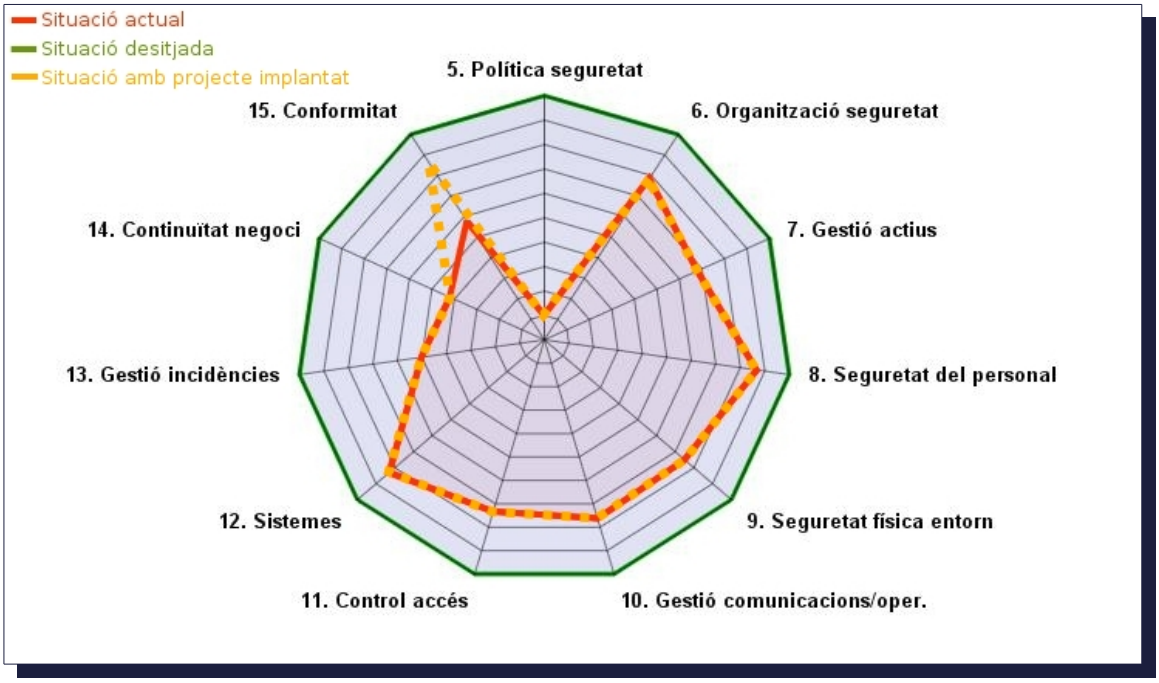

Figura 7-11: Diagrama radar del compliment ISO amb el PROJ-PROC-011

7.4.2 REVISIÓ I MILLORA DE LES POLÍTIQUES D'*ACTIVE DIRECTORY* (DOMINI)

Els recursos de la xarxa i les polítiques dels diferents usuaris per les estacions de treball

que utilitzen s'apliquen des de l'*Active Directory* del domini actual. Aquestes polítiques permeten la gestió dels canvis de contrasenyes, alta/baixa d'usuaris, assignació a grups, creació d'unitats organitzatives, tancar sessió, configurar el comportament de les estacions de treball, definir horaris de connexió en màquines, etc.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-012**
NOM:	**REVISIÓ I MILLORA DE LES POLÍTIQUES D'ACTIVE DIRECTORY**
OBJECTIUS:	- Millora de les polítiques aplicades actualment per Active Directory. - Implantació de procés de revisió i millora periòdic.
ABAST:	- Departament TIC: Windows 2008 Domain Server.
DESCRIPCIÓ:	- Revisió de les polítiques aplicades actualment als diferents usuaris/grups per tal de detectar possibles anomalies o millores en aspectes relacionats amb la seguretat com pot ser la complexitat de les contrasenyes, els *timeouts* de sessió, horaris de connexió a màquines, etc. - Definició d'un procediment de revisió i millora periòdic per tal de mantenir i seguir millorant les polítiques que s'apliquen.
ACTIVITATS:	- Revisió del sistema actual. - Aplicació de millores. - Definició de procediment de revisió i millora periòdic.
BENEFICIS:	- Millora de la seguretat dels recursos compartits. - Millora de la seguretat de certs aspectes de les estacions de treball.
COST ECONÒMIC:	**2.000 €**.
TEMPS EXECUCIÓ:	**4 mesos**
AFECTACIÓ AARR:	- Millores evidents vers l'actiu **[SW.17]** (Sistemes operatius d'estacions de treball), sobretot per les amenaces del tipus [A] (atacs intencionats) i en menor mesura del tipus [E] (errors no intencionats).
AFECTACIÓ ISO:	**- 11 Control d'accés:** Afectaria diferents objectius de control del domini 11, referents a desconnexions de sessió, gestió de

	contrasenyes, restriccions d'accés, etc.

Taula 7-12: Projecte PROJ-012

El diagrama de compliment de la ISO es mostra en el diagrama de la *Figura 7-12*. S'hi pot observar com el percentatge de compliment s'eleva del 73,54% al 83,75%.

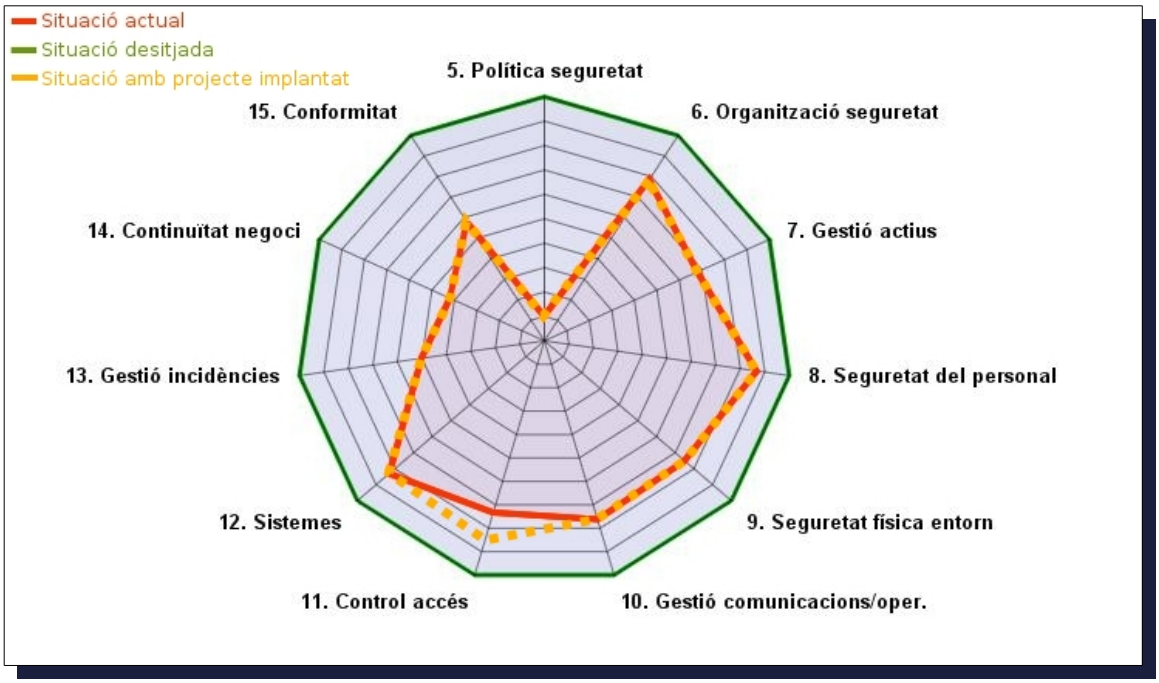

Figura 7-12: Diagrama radar del compliment ISO amb el PROJ-PROC-012

7.4.3 REESTRUCTURACIÓ DEL DEPARTAMENT TIC

En l'anàlisi de riscos realitzat apareix un risc elevat en l'apartat de personal tècnic. Això és degut a un risc en la disponibilitat de l'actiu. Analitzant el cas, es pot comprovar com la causa és la freqüent amenaça de no disponibilitat del personal. Analitzant el organigrama de l'Ajuntament de Riberola es pot arribar a la conclusió de el Departament de Tecnologies de la Informació i la Comunicació no disposa dels recursos humans suficients per la realització correcta de les tasques assignades, donat el volum d'elements actual de l'organització.

Les dades bàsiques del projecte es presenten en la següent taula:

REFERÈNCIA:	**PROJ-013**
NOM:	**REESTRUCTURACIÓ DEL DEPARTAMENT DE TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ**

OBJECTIUS:	- Contractar un tècnic de sistemes per manteniment de la microinformàtica, o contracte de serveis amb empresa externa per la realització de tasques de microinformàtica i atenció als usuaris, així com poder realitzar substitucions temporals d'altres membres del departament.
ABAST:	- Departament de Tecnologies de la Informació i la Comunicació.
DESCRIPCIÓ:	- Es desitja contractar un tècnic o el servei d'una empresa externa per la realització de tasques de microinformàtica i atenció als usuaris per tal de reduir la càrrega laboral del personal actual. - Amb aquesta acció, es desitja que els recursos humans del Departament TIC actual estiguin en disposició d'emprar més hores en projectes referents a seguretat, documentació i definició de procediments.
ACTIVITATS:	- Contractació (nou empleat o empresa externa) - Període d'adaptació i proves - Definició exacta de funcions del personal del departament.
BENEFICIS:	- Millora del servei d'atenció a l'usuari actual. - Millora de la resta de funcions degut a augment de recursos disponibles.
COST ECONÒMIC:	**34.000 €** (anuals)
TEMPS EXECUCIÓ:	**6 mesos**
AFECTACIÓ AARR:	L'amenaça *Indisponibilitat del personal* [E.28] es redueix de manera considerable sobre els actius [P.2] i [P.3]. Això provoca que ja no presentin un risc elevat un cop implementat el projecte.
AFECTACIÓ ISO:	**- Sense afectació directa:** No existeix una afectació directa, tot i que a la llarga el poder disposar de més recursos redundarà en una millora de certs procediments. Per tant, es preveu una millora en certs punts indirectament en la següent auditoria o revisió.

Taula 7-13: Projecte PROJ-013

No hi ha cap variació de manera directa en el digrama de compliment ISO mitjançant l'execució d'aquest projecte.

7.5 RESUM I CONCLUSIONS

Un cop definits tots els projectes planificats per cadascun dels períodes, podem realitzar un resum de la planificació de cadascun dels tres anys, així com de les despeses que hauria de realitzar l'organització.

Es valorarà quin seria l'estat final del compliment dels diferents dominis de la ISO 27001 respecte l'estat actual un cop aplicats els diferents projectes, i quina afectació implicaria respecte l'anàlisi de riscos realitzat en el present document.

L'anàlisi diferencial realitzat en el punt 4 ha determinat en quins punts l'organització no disposava de controls ni procediments suficients per complir de manera suficient amb l'estàndard ISO 27000. D'altra banda, l'anàlisi de riscos realitzat en l'apartat 6.6 ens indica quins actius de l'organització estan més exposats a riscos, ja sigui per l'alt impacte que suposaria veure l'actiu afectat per una amenaça, com també per l'alta freqüència de materialització d'aquesta amenaça. Aquests dos anàlisis han permès definir un número de projectes a realitzar per tal de millorar la seguretat en les tecnologies de la informació i la comunicació, adaptant els seus procediments a la ISO 27000 i reduint el risc dels actius més valuosos que estaven exposats.

7.5.1 PLANIFICACIÓ DELS PROJECTES AL LLARG DELS TRES ANYS

En la realització de la planificació s'ha tingut en compte de no executar més de dos projectes a la vegada, per poder gestionar millor la seva evolució.

La planificació definida per l'execució dels diferents projectes, dividida pels tres anys de durada es presenta en la *Taula 7-14*.

PROJECTES PRIMER ANY	1	2	3	4	5	6	7	8	9	10	11	12
PROJ-001 Adquisició de programari antivirus corporatiu												
PROJ-002 Procediments d'actualitzacions de sistemes operatius												

PROJ-003 Documentació/Implantació de Polítiques de Seguretat												
PROJ-004 Realització de l'inventari d'actius												
PROJ-005 Millora de climatització en els CPD												
PROJ-006 Revisió de procediments en Recursos Humans												
PROJECTES SEGON ANY	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
PROJ-007 Formació del personal en seguretat de les TIC												
PROJ-008 Gestió d'incidències – Programari i procediments												
PROJ-009 Definició de plans de continuïtat												
PROJ-010 Definició de procediments de còpies de seguretat												
PROJECTES TERCER ANY	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
PROJ-011 Formació del personal en seguretat de les TIC												
PROJ-012 Gestió d'incidències – Programari i procediments												
PROJ-013 Definició de plans de continuïtat												

Taula 7-14: Planificació dels diferents projectes durant els tres pròxims anys

Durant els últims tres mesos del tercer any es deixa un període sense projectes programats per a poder gestionar possibles retrocessos en el desenvolupament d'algun dels projectes.

7.5.2 ESTIMACIÓ ECONÒMICA

Les despeses a realitzar per part de l'organització per cadascun dels períodes es resumeix en la *Taula 7-15*.

PROJECTES PRIMER ANY	COST
PROJ-001 Adquisició de programari antivirus corporatiu	2.500,00 €
PROJ-002 Procediments d'actualitzacions de sistemes operatius	0,00 €
PROJ-003 Documentació/Implantació de Polítiques de Seguretat	5.500,00 €
PROJ-004 Realització de l'inventari d'actius	500,00 €
PROJ-005: Millora de climatització en els CPD	12.000,00 €
PROJ-006 Revisió de procediments en Recursos Humans	500,00 €
TOTAL:	**21.000,00 €**
PROJECTES SEGON ANY	**COST**
PROJ-007 Formació del personal en seguretat de les TIC	5.000,00 €
PROJ-008 Gestió d'incidències – Programari i procediments	12.700,00 €
PROJ-009 Definició de plans de continuïtat	1.000,00 €
PROJ-010 Definició de procediments de còpies de seguretat	1.500,00 €
TOTAL:	**20.200,00 €**
PROJECTES TERCER ANY	**COST**
PROJ-011 Formació del personal en seguretat de les TIC	25.000,00 €
PROJ-012 Gestió d'incidències – Programari i procediments	2.000,00 €
PROJ-013 Definició de plans de continuïtat	34.000,00 €
TOTAL:	**61.000,00 €**

Taula 7-15: Despeses per projecte i any

D'altra banda, s'han deixat els dos projectes que suposen més despesa per l'últim any, de manera que l'Ajuntament disposi del temps necessari per poder-hi assignar les partides pressupostàries necessàries per la seva execució.

7.5.3 IMPACTE DELS PROJECTES EN L'ANÀLISI DE RISCOS

A la finalització dels tres anys, havent-se executat correctament tots els projectes, haurem mitigat el risc pels deu actius amb risc més elevat de l'organització (veure *Figura 6-3*). Per tant, el següent anàlisi de riscos ens s'espera que mostri uns resultats totalment diferents als actuals (diferents actius amb risc màxim, però en un risc menor), permetent-nos millorar el risc dels actius en cada cicle PDCA del Sistema de Gestió de Seguretat de la Informació.

7.5.4 IMPACTE DELS PROJECTES EN EL COMPLIMENT DE LA ISO 27001

L'impacte global dels diferents projectes en conjunt respecte el compliment actual es pot observar en el diagrama de la *Figura 7-13*. Analitzant el diagrama s'observa com mitjançant els projectes definits, l'organització aconsegueix acostar-se a uns nivells elevats de compliment per tots els dominis de la ISO, sempre per sobre del 75%.

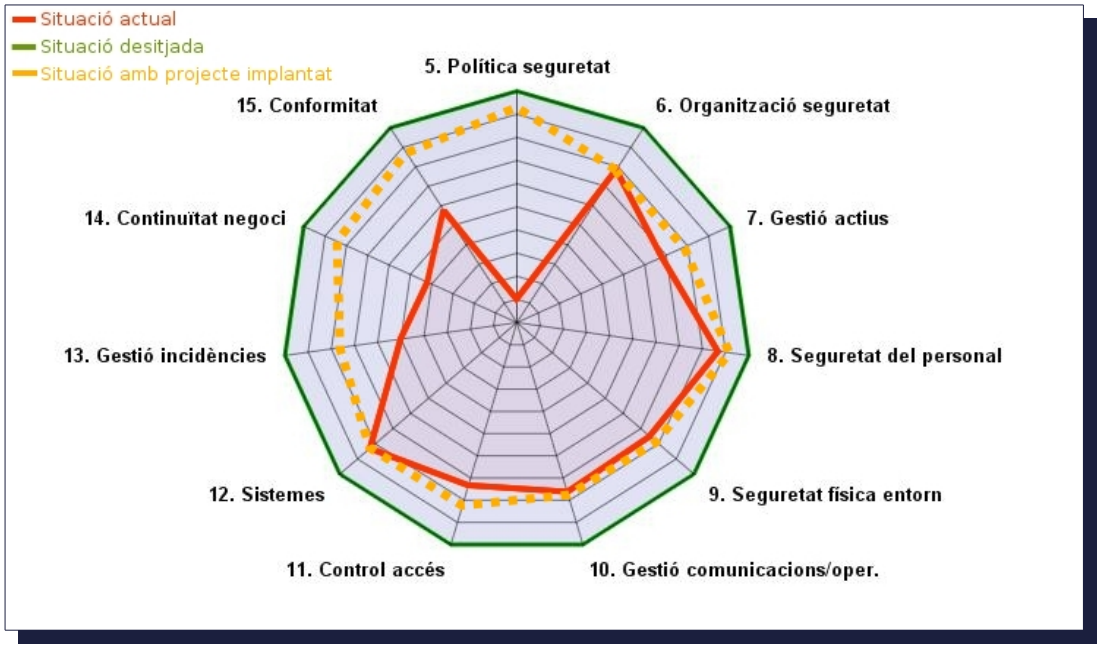

Figura 7-13: Compliment de la ISO un cop executats els diferents projectes

Tal i com es pot veure en el diagrama, s'ha volgut potenciar l'execució de projectes que permetessin implementar controls en dominis que fins ara no estaven massa contemplats com la Gestió d'incidències (13), la continuïtat del negoci (14), la Conformitat (15) o la política de seguretat (5). Tot i així, també s'han vist afectats la major part dels altres dominis, tot i que de manera menys significativa, ja que segons la valoració dels diferents nivells de maduresa establerts per aquest projecte, a nivells alts la puntuació difereix molt menys que en els nivells inicials. Això implica que al pujar els primers nivells de

maduresa, la puntuació s'incrementa molt més que no pas al augmentar de nivell en els més alts.

8. AUDITORIA DE COMPLIMENT

8.1 INTRODUCCIÓ

Arribats en aquest punt, es realitzarà una avaluació exhaustiva de fins a quin punt l'organització compleix amb les bones pràctiques en matèria de seguretat. La ISO/IEC 27002:2005 ens servirà com a marc de referència pel control de l'estat de la seguretat.

Tal i com s'ha comentat anteriorment, la ISO/IEC 27002:2005 agrupa un total de 133 controls o mesures preventives sobre bones pràctiques per a la Gestió de la Seguretat de la Informació. Aquests 133 controls estan organitzats en 11 àrees o dominis, que alhora es divideixen en 39 objectius de control. És un estàndard reconegut a nivell mundial i és perfectament vàlid per la majora de les entitats, empreses o organitzacions que precisin de Sistemes de Gestió de Seguretat de la Informació.

Els controls de la ISO/IEC 27002:2005, o els de qualsevol altre catàleg o metodologia similar, tracten diferents aspectes, entre els que destaquen:

- Formalització de les bones pràctiques mitjançant documents escrits o aprovats.
- Política de personal.
- Sol·licituds tècniques (programari, maquinari o comunicacions).
- Seguretat física o d'entorn.

Per tant, l'objectiu d'aquesta auditoria és avaluar la maduresa de la seguretat en relació als diferents dominis de control, objectius de control i 133 controls que planteja la ISO/IEC 27002:2005.

Els diferents valors que atorgarem a cadascun dels 133 controls venen determinats pel model de maduresa de la capacitat CMM, que es poden consultar en la *Taula 4-2* del present document, en el capítol *"4. Anàlisi diferencial"*, on es mostra un resum del resultat de l'auditoria del compliment. A diferència de l'anàlisi diferencial, aquesta auditoria mostrarà les anotacions corresponents per les diferents no conformitats majors i menors detectades en els diferents controls, així com les diferents observacions a realitzades.

En l'Annex A3 es poden consultar diferents plantilles de documents per tal de documentar les diferents no conformitats i observacions resultat de les auditories de compliment que es puguin realitzar al llarg del temps. Per tant, tot i que en aquest apartat es presentarà una taula amb les diferents no conformitats i observacions, cal destacar que per cadascuna

caldria assignar una fitxa en la qual es realitzaria el seguiment d'aquesta no conformitat o observació.

8.2 AUDITORIA DE COMPLIMENT

La *Taula 8-1* conté el resum dels resultats dels diferents objectius de control respecte l'auditoria de compliment realitzada. S'hi esmenten les diferents no conformitats detectades, així com observacions o comentaris al respecte.

5. POLÍTICA DE SEGURETAT	**10,00%**
5.1 Política de seguretat de la informació	**10%**
5.1.1 Document de política de seguretat *	L1 - 10%
NO CONFORMITATS MAJORS: NC01. **COMENTARIS:** El document de política de seguretat és molt limitat, i no té en compte molts punts necessaris per a considerar-ho com a tal. A més, manca l'aprovació per part de direcció, tot i que es fa molt de tant en tant. S'atorga nivell L1 degut a que la política de seguretat, tot i que precària i incompleta, existeix. Per tant, es considera que est troba en un estat inicial. Cal destacar que es tracta d'un control obligatori per tal de complir amb la norma ISO/IEC 27001:2005.	
5.1.2 Revisió de la política de seguretat	L1 - 10%
NO CONFORMITATS MAJORS: NC01. **COMENTARIS:** El document de política de seguretat és molt limitat i no existeix procés de revisió, tot i que es fa molt de tant en tant. S'atorga nivell L1 perquè la revisió de l'existent es realitza, tot i que sense un període fixat i molt poc freqüentment.	
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ	**73,03%**
6.1 Organització interna	**69,38%**
6.1.1 Comitè de seguretat	L1 - 10%
NO CONFORMITATS MAJORS: NC01. **COMENTARIS:** El document de política de seguretat és molt limitat, i això afecta l'organització interna. S'hi esmenta un nivell de direcció però no el	

defineix exactament com a Comitè de Seguretat, ni les funcions són exactament les mateixes. S'atorga nivell L1 a falta de corregir-ho.

6.1.2 Coordinació	L2 - 50%

NO CONFORMITATS MAJORS: NC01.

COMENTARIS: Existeix certa coordinació, però fins ara no era massa oficial ni seguint cap procediment concret. S'atorga nivell L2 perquè es troba en un nivell inicial, però li falta molt per millorar. S'espera que la implantació de la nova política present en aquest document permeti un augment considerable del nivell de maduresa d'aquest control.

6.1.3 Assignació de responsabilitats *	L3 - 90%

NO CONFORMITATS MENORS: NC02.

COMENTARIS: Hi ha certes deficiències i incongrüències en alguns dels càrrecs, i alguns departaments o càrrecs no tenen molt determinades algunes de les seves funcions. Faltaria documentar exactament les funcions. S'assiga un nivell L3. Cal destacar que és un control necessari per la ISO/IEC 27001:2005.

6.1.4 Autorització de recursos	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: L'assignació de recursos, sobretot econòmics, està degudament regulat pel departament d'intervenció, que realitza un control exhaustiu i documentat de les diferents despeses dels departaments, per tal que estiguin dins dels pressupostos anuals.

6.1.5 Acords de confidencialitat	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: Durant la contractació, el Departament de Secretaria de l'Ajuntament s'encarrega de velar que els contractin diposin de les clàusules adients. A més, tots els contractes o convenis romanen degurament documentats en un gestor d'expedients.

6.1.6 Contacte amb autoritats	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: El contacte amb diferents autoritats està degudament regulat mitjançant els diferents registres d'entrada i sortida, així com el gestor d'expedients. A més, l'Ajuntament disposa del Cos de Policia Municipal, el qual està en contacte amb altres cossos policials.

6.1.7 Contacte amb altres grups d'interès	L4 - 95%

OBSERVACIONS: OBS01

COMENTARIS: El contacte amb altres grups d'interès sempre depén dels diferents departaments, però qualsevol conveni o contracte queda degudament documentat, així com revisat per part de secretaria.

6.1.8 Revisió independent	L1 - 10%

NO CONFORMITATS MAJORS: NC03.

COMENTARIS: No existeixen revisions independents realitzades per tercers respecte el SGSI ni la seva impantació. Cal realitzar una planificació d'auditories o consultories externes per tal de produir aquesta revisió per tercers.

6.2 Tercers	**76,67%**
6.2.1 Identificació de recursos	L3 - 90%

NO CONFORMITATS MENORS: NC04.

COMENTARIS: En alguns casos no s'ha realitzat correctament quins recursos són a l'abast d'alguns tercers. Caldria revisar possibles contractes de serveis o convenis per establir-los formalment.

6.2.2 Seguretat en la relació amb clients	L2 - 50%

NO CONFORMITATS MENORS: NC04.

COMENTARIS: De la revisió d'un cert nombre de contractes/convenis de l'Ajuntament de Riberola amb tercers se'n desprén que algun aspecte relatiu a la seguretat no està plenament contemplat.

6.2.3 Seguretat en acords amb terceres parts	L3 - 90%

NO CONFORMITATS MENORS: NC04.

COMENTARIS: Algun aspecte relatiu a la seguretat no està complet. Cal ser més exhaustiu a l'hora d'elaborar els contractes/convenis en matèira de seguretat de la informació. Tot i així certes parts es consideren correctes i Secretaria ho té en compte sempre. Per tant, està definit, només cal completar-ho (Nivell L3).

7. GESTIÓ D'ACTIUS	**68,75%**
7.1 Responsabilitats sobre els actius	**65,00%**
7.1.1 Inventari d'actius	L2 - 50%

NO CONFORMITATS MAJORS: NC05.

COMENTARIS: L'inventari d'actius no està correctament actualitzat. No existeixen procediments de manteniment/alta/baixa formals, cosa que facilita que no estigui constantment actualitzat. Per tant, existeix però no funciona com hauria. Es puntua com a L2.

7.1.2 Propietat dels actius	L4 - 95%

OBSERVACIONS: OBS02

COMENTARIS: La propietat dels actius està correctament definida. Cada departament sap de quins actius és responsable, tot i que l'accés a alguns actius sigui compartit. Potser falta alguna documentació addicional, però en general està correcte. Nivell L4.

7.1.3 Ús acceptable dels actius	L2 - 50%

NO CONFORMITATS MAJORS: NC05.

COMENTARIS: No sempre s'utilitzen correctament els actius. S'han detectat numerses incidències en certes tipologies d'actius que susggereixen un mal ús per desconeixement per part de l'usuari.

7.2 Classificació de la Informació	**72,50%**

7.2.1 Guies de classificació	L4 - 95%

OBSERVACIONS: OBS02

COMENTARIS: La informació es pot classificar segons la seva confidencialitat, valor i sensibilitat, tot i que cada departament ho fa amb el seu procediment particular. Seria bò que fós un procediment a nivell d'organització. Per tant, nivell L4.

7.2.2 Marcatge i tractament de la informació	L2 - 50%

NO CONFORMITATS MAJORS: NC05.

COMENTARIS: Tot i exisitir procediments per a realitzar la classificació de la informació, s'ha observat docoumentació classificada sobre de les taules, o en llocs compromesos. Podria ser degut a falta de formació respecte els procediments de marcatge i tractament. Tot i així no sempre succeeix.

8. SEGURETAT RELATIVA AL PERSONAL	**91,11%**
8.1 Abans de la contractació	**93,33%**
8.1.1 Rols i responsabilitats	L3 - 90%

NO CONFORMITATS MENORS: NC06.

COMENTARIS: Dins L'organització podem trobar una correcta assignació de responsabilitats, donat que al tractar-se d'una administració pública els diferents càrrecs estan estipulats de manera oficial: administratiu, auxiliar, tècnic, cap de departament, etc. Tot i així, existeixen certes deficiències i incongrüències en alguns dels càrrecs, i alguns departaments o càrrecs no tenen molt determinades algunes de les seves funcions. Faltaria documentar exactament les funcions. S'assiga un nivell L3.

8.1.2 Selecció i política de personal	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: La selecció i política de personal és mitjançant oposició, ja que l'administració pública té l'obligació de fer-ho així. Per tant, és públic i transparent sempre i quan no es tracti de càrrecs de confiança i polítics.

8.1.3 Termes i condicions de la relació laboral	L3 - 90%

NO CONFORMITATS MENORS: NC06.

COMENTARIS: Tot i que la majoria dels càrrec concorden amb les funcions que realitza el treballador, s'han detectat casos on no hi ha coherència entre classe de treballador i funcions que desenvolupa. Caldria evitar aquest tipus de casos.

8.2 Durant la relació laboral	**80,00%**
8.2.1 Supervisió d'obligacions	L3 - 90%

NO CONFORMITATS MENORS: NC06.

COMENTARIS: Els caps realitzen una supervisió de les obligacions dels diferents treballadors, així com el Regidor de Personal supervisa el funcionament dels diferents departaments. La major part dels casos estan ben resolts, però no es deixa constància per escrit dels resultats de les diferents supervisions, així com de possibles incidències.

8.2.2 Conscienciació, formació i capacitació en seguretat *	L2 - 50%

NO CONFORMITATS MAJORS: NC05.

COMENTARIS: La formació periòdica de seguretat es limita a la seguretat física. En el cas de l'Ajuntament de Riberola, no s'efectuen formacions a nivell de seguretat de la informació. Els conceptes i procediments són explicats en els diferents departaments pels respectius caps, mentre que certs conceptes són comentats pel departament de les TIC. Caldria formalitzar i planificar formacions.

8.2.3 Procediment disciplinari	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: El procediment disciplinari està estipulat en l'estatut bàsic del treballador públic en l'àmbit de l'administració local. Per tant, està establert i documentat perfectament, a més d'estar a l'abast de tothom.

8.3 En finalitzar la contractació o canvi d'ocupació	**100.00%**
8.3.1 Cessació de responsabilitats	L5 - 100%

OBSERVACIONS: OBS03

COMENTARIS: La cessació de responsabilitats segueix un procediment establert de manera correcta, tant per treballadors com per càrrecs polítics.

8.3.2 Devolució d'actius	L5 - 100%

OBSERVACIONS: OBS03

COMENTARIS: La devolució d'actius està correctament gestionada en part pels procediments de personal corresponents, i en gran part també perquè el punt *7.1.2 Propietat dels actius* està en un nivell de compliment elevat (L4).

8.3.3 Eliminació de drets d'accés	L5 - 100%

OBSERVACIONS: OBS03

COMENTARIS: Gestionat correctament pel departament de personal. Comunicació als departaments corresponents per eliminar corresponents drets d'accés. Documentació i registre de notificacions (en correu electrònic). Nivell L5.

9. SEGURETAT FÍSICA I DE L'ENTORN	**77,23%**
9.1 Àrees segures	**83,75%**
9.1.1 Perímetre de seguretat física	L3 - 90%

NO CONFORMITATS MENORS: NC07.

COMENTARIS: Els elements que contenen informació o els diferent equips necessaris per consultar-la estan tots dins les diferents dependències de l'organització. De totes maneres, algunes de les seus han patit algun robatori de menor importància durant els últims mesos. Cal realitzar les actuacions necessàries per evitar aquest tipus de robatoris.

9.1.2 Control d'accés físic	L5 - 100%

OBSERVACIONS: OBS04

COMENTARIS: Els accessos a dependències amb informació sensible com despatxos i CPDs disposen de pany amb clau per evitar accessos no autoritzats.

La Policia Municipal disposa de claus i d'un registre en cas que s'hagi de cedir a algun tercer, sempre mitjançant la pertinent autorització.

9.1.3 Seguretat en oficines, despatxos i recursos	L4 - 95%

OBSERVACIONS: OBS04

COMENTARIS: Els accessos a dependències amb informació sensible com despatxos i CPDs disposen de pany amb clau per evitar accessos no autoritzats. La Policia Municipal disposa de claus i d'un registre en cas que s'hagi de cedir a algun tercer, sempre mitjançant la pertinent autorització.

9.1.4 Protecció enfront d'amenaces externes i d'entorn	L2 - 50%

NO CONFORMITATS MENORS: NC08.

COMENTARIS: Els diferents CPD no disposen de controls de temperatura i humitat, considerat com el mínim necessari per gestionar el seu correcte funcionament. Tot i així, existeixen extintors, alarmes d'incendis i fums a la major part de les seus, i els CPD disposen d'aire acondicionat.

9.1.5 El treball en àrees segures	N/A

NO APLICA.

9.1.6 Accés públic, zones de càrrega i descàrrega	N/A

NO APLICA.

9.2 Seguretat en equips	**70,71%**
9.2.1 Ubicació i protecció	L4 - 95%

OBSERVACIONS: OBS05

COMENTARIS: Els diferents equips es troben dins les diferents dependències, les quals diposen de recepció durant l'horari d'atenció al client, i fora d'horari es tanquen. La Policia Municipal vigila les diferents dependències i es disposa d'algunes càmeres IP de video vigilància per tal de tenir un mínim control de les diferents seus.

9.2.2 Subministraments	L5 - 100%

OBSERVACIONS: OBS05

COMENTARIS: El subministrament elèctric al sismta principal queda garantit per diferents sistemes d'alimentació ininterrompuda als diferents CPD.

9.2.3 Seguretat del cablejat	L5 - 100%

OBSERVACIONS: OBS05

COMENTARIS: El cablejat ethernet està sempre dins la paret dins de tubs corrugats, o en alguns casos puntuals cobert per canaleta de plàstic. En el cas de la fibra òptica, sempre es passa soterrada menys algun cas puntual on s'ha hagut de grapar per façana. Els canvis de nivell la fibra òptica disposa de tubs d'acer o alumini per evitar possibles manipulacions.

9.2.4 Manteniment dels equips	L3 - 90%

NO CONFORMITATS MENORS: NC10.

COMENTARIS: Detecció d'un nombre no massa elevat de sistemes amb problemes: sistema anticuat, infecció de codi maliciós o actualitzacions de seguretat sense aplicar. En el cas dels aires acondicionats i altres equips auxiliars (per exemple extintors i alarmes), existeix procediment de revisió periòdic.

9.2.5 Seguretat fora dels locals	L0 - 0%

NO CONFORMITATS MAJORS: NC08.

COMENTARIS: La formació dels empleats és bàsica. Dels diferents ordinadors portàtils analitzats, en cap s'estava realitzant un xifratge de la informació. En cas de pèrdua o robatori, la informació es veuria compromesa, mentre que si està xifrada correctament, la seva confidencialitat estaria garantida.

9.2.6 Reutilització o eliminació	L5 - 100%

OBSERVACIONS: OBS05

COMENTARIS: Es realitza el reciclatge correcte dels diferents equipaments,

així com l'eliminació o destrucció completa dels elements que poden contenir dades.

9.2.7 Autorització de sortida	L1 - 10%

NO CONFORMITATS MAJORS: NC08.

COMENTARIS: Es sol·licita un permís verbal, i de manera molt informal per la sortida de segons quins elements. No existeix un control respecte alguns dispositius com memòries USB. Es precisa autorització per escrit i un control més exhaustius respecte dispositius extraïbles.

10. GESTIÓ DE COMUNICACIONS I OPERACIONS	**85,22%**
10.1 Procediments d'operació i responsabilitats	**66,66%**
10.1.1 Documentació de procediments	L0 - 0%

NO CONFORMITATS MAJORS: NC11.

COMENTARIS: No exsiteix o en alguns casos es mostra insuficient. Només l'Oficina d'Atenció al Ciutadà segueix procediments escrits, però la resta de departaments no tenen cap documentació al respecte.

10.1.2 Gestió de canvis	L1 - 10%

NO CONFORMITATS MAJORS: NC11.

COMENTARIS: No exsiteix cap documentació ni gestió dels canvis realitzats, però si que s'aporta cert grau de documentació, insuficient per poder-lo anomenar gestió de canvis, però que pot servir com a embrió per iniciar una gestió de canvis apropiada.

10.1.3 Segregació de funcions	L4 - 95%

NO CONFORMITATS MENORS: NC02.

COMENTARIS: Les diferents funcions en els procediments d'operació i responsabilitats estan ben definits, degut a la mida del departament TIC. Tot i així, no estan documentades i en altres departaments no queda tan clar.

10.1.4 Separació d'entorns desenvolupament i producció	L4 - 95%

OBSERVACIONS: OBS08

COMENTARIS: En els casos necessaris, es generen un mínim de dos entorns, un per poder realitzar les diferents proves i l'altre el de producció.

10.2 Gestió de la prestació de serveis per tercers	**93,33%**
10.2.1 Prestació de serveis	L4 - 95%

OBSERVACIONS: OBS01

COMENTARIS: Les diferents garanties de seguretat, definicions dels diferents serveis i nivells d'entrega dels diferents serveis sempre queden correctament estipulats en els diferents convenis o contractes que l'administració signa amb els diferents tercers amb els que tracta.

10.2.2 Monitoratge i revisió de serveis	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: El monitoratge dels diferents serveis es realitza mitjançant l'eina Nagios, podent definir diferents periodicitats de comprovacions. Existeix la possibilitat de realitzar les notificacions d'esdeveniments importants mitjançant SMS. Els serveis de tercers són o pàgines web (monitorització habilitada tant del host com del servei HTTP) o interns (monitorització parametrizada segons la necessitat).

10.2.3 Gestió de canvis en els serveis	L3 - 90%

NO CONFORMITATS MENORS: NC12.

COMENTARIS: Degut a l'alt volum de feina, els diferents canvis en els serveis no es veuen immediatament reflexats en les diferents documentacions o registres, així com en els sistemes de monitoratge.

10.3 Planificació i acceptació del sistema	**100%**
10.3.1 Gestió de la capacitat	L5 - 100%

OBSERVACIONS: OBS07

COMENTARIS: Nagios és capaç de monitoritzar diferents serveis, tant externs

com interns dels propis servidors. Per tant, des de Nagios es monitoritza i emmagatzema la informació respectiva a ús de capacitat de disc, memòria i processador del diferent maquinari per tal de poder-ho controlar. Es generen alertes, que poden aportar un control per la gestió de la capacitat de manera senzilla i automàtica.

10.3.2 Acceptació de sistemes	L5 - 100%

OBSERVACIONS: OBS07

COMENTARIS: S'estableixen criteris d'acceptació per a nous sistemes d'informació, actualització i versions noves. Existeixen procediments per tal de realitzar aquestes modificacions. Sempre es defineixen periodes de prova per tal de poder validar els canvis o nous sistemes a implementar.

10.4 Protecció conta codi maliciós	**92,50%**
10.4.1 Protecció contra codi maliciós	L3 - 90%

NO CONFORMITATS MENORS: NC10.

OBSERVACIONS: OBS07

COMENTARIS: Certa seguretat és aportada per elements o serveis de xarxa que eviten certa propagació o execució d'elements de xarxes externes, així com la seva possible detecció i tractament (IDS). D'altra banda, no disposar d'un antivirus amb el que poder controlar el número d'infeccions determina la valoració d'aquest control com a L3.

10.4.2 Protecció contra codi descarregat en el client	L4 - 95%

NO CONFORMITATS MENORS: NC10.

OBSERVACIONS: OBS06

COMENTARIS: Les polítiques actuals d'Active Directory no permeten a l'usuari la instal·lació de certs programes. Tot i així la no conformitat és degut a que no hi ha desplegat un antivirus de manera integrada, que permeti detectar o evitar l'execució de cert codi maliciós.

10.5 Gestió de suports i recuperació	**100%**
10.5.1 Recuperació de la informació	L5 - 100%

OBSERVACIONS: OBS07

COMENTARIS: L'Ajuntament disposa d'una unitat robòtica que gestiona la recuperació de la informació i les còpies de seguretat en cinta dels diferents servidors de l'Ajuntament. A més, també es diposa de còpies de les imatges dels diferents sistemes virtuals per possibles recuperacions ràpides de sistema. Es registren les diferents còpies i es fan proves setmanals de restauració de dades.

10.6 Gestió de la seguretat de xarxes	**100%**
10.6.1 Controls de xarxa	L5 - 100%

OBSERVACIONS: OBS06, OBS07

COMENTARIS: Nagios, l'IDS, tallafocs i Active Directory amb la seva gestió d'usuaris proporcionen diferents capes de seguretat a l'hora d'accedir als serveis de xarxa oferts per l'organització. Tots aquests elements propocionen suficients registers per portar un control del nombre d'incidències generades en un període determinat de temps.

10.6.2 Seguretat dels serveis de xarxa	L5 - 100%

OBSERVACIONS: OBS06, OBS07

COMENTARIS: Els diferents serveis de xarxa com el tallafocs i el proxy, així cmo el controlador de domini mitjançant Active Directory proporcionen diferents capes de seguretat a l'hora d'accedir als serveis de xarxa oferts per l'organització. Els intents d'accés incorrecte i altres incidències queden registrades per tal de poder-ne portar un control.

10.7 Gestió de suports d'informació	**53,75%**
10.7.1 Gestió de suports extraïbles	L1 - 10%

NO CONFORMITATS MAJORS: NC09.

COMENTARIS: La gestió dels diferents suports extraïbles amb els que treballa l'organització no diposa de cap tipus de procediment central. En algun cas, algun departament, però molt aïllat.

10.7.2 Retirada de suports	L4 - 95%

OBSERVACIONS: OBS05

COMENTARIS: Es realitza el reciclatge correcte dels diferents equipaments, així com l'eliminació o destrucció completa dels elements que poden contenir dades.

10.7.3 Procediments d'utilització de la informació	L1 - 10%

NO CONFORMITATS MAJORS: NC11.

COMENTARIS: En la majora part dels casos no existeixen o es mostren insuficients per a que siguin útils.

10.7.4 Seguretat en la documentació dels sistemes	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: El controlador de domini, mitjançant Active Directory i la seva gestió d'usuaris, proporcionen diferents capes de seguretat a l'hora d'accedir als serveis de xarxa oferts per l'organització. Un d'aquests serveis és el servidor de fitxers.

10.8 Intercanvi d'informació	**61,00%**
10.8.1 Polítiques i procediments d'intercanvi d'informació	L1 - 10%

NO CONFORMITATS MAJORS: NC11.

COMENTARIS: No existeixen formalment, tot i que evidentment s'estableixen per necessitat. Carència evident i per tant se li assigna L1.

10.8.2 Acords d'intercanvi	L4 - 95%

OBSERVACIONS: OBS01

COMENTARIS: L'Ajuntament ha de realitzar acords o convenis per escrit, els quals porten sempre el vist i plau de Secretaria i Intervenció, així com de la Junta de Govern Local, que és l'órgan que aprova la signatura o no de l'acord. S'exigeix la signatura d'aquest tipus d'acord en aquests casos, tot i que revisant la informació actual alguns contractes realitzats no ho contemplen.

10.8.3 Suports físics en trànsit	L1 - 10%

NO CONFORMITATS MAJORS: NC09.

COMENTARIS: No existeixen formalment un procés d'autorització de sortida d'aquests suports, però es defineix que es troba en un nivell inicial perquè existeix un procediment de registre de sortida i d'enviament certificat segons el tipus d'enviament i de suport. De totes maneres en molts casos no se'n fa ús exhaustiu i es porta en mà.

10.8.4 Missatgeria electrònica	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: El servidor de correu, així com els diferents correus electrònics corporatius es troben en un sistema intern. Es disposa de control antispam i antivirus per tal de fer més segur el correu. Les comunicacions amb el servidor són xifrades (SSL).

10.8.5 Sistemes d'informació del negoci	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: L'Ajuntament disposa d'una unitat robòtica que gestiona la recuperació de la informació i les còpies de seguretat en cinta dels diferents servidors de l'Ajuntament. També es realitzen còpies de les imatges dels diferents sistemes virtuals per possibles recuperacions ràpides de sistema. Altres sistemes com tallafocs, proxy, IDS i nagios ofereixen seguretat addicional, tant de manera activa com passiva.

10.9 Serveis de comerç electrònic	**100%**
10.9.1 Comerç electrònic	N/A

NO APLICA.

10.9.2 Transaccions en línia	N/A

NO APLICA.

10.9.3 Informació d'accés públic	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: Al tractar-se d'una administració pública local, l'Ajuntament està en l'obligació de posar a disposició del ciutadà certa informació pública. Alguna, inclús amb la necessitat de poder-ne demostrar la disponibilitat i el segellat de temps i autenticitat. S'empra un perfil del contractant per casos molt específics i amb aquests requeriments, i una pàgina web pública per la resta d'informació menys crítica.

10.10 Monitoratge	**85,00%**
10.10.1 Registre d'activitats	L3 - 90%

NO CONFORMITATS MENORS: NC14.

COMENTARIS: Gestió poc centralitzada, ja que cada sistema emmagatzema les seves. En tot cas l'únic registre general existent actualment és el IDS, ja que processa el tràfic de xarxa.

10.10.2 Ús dels sistemes de monitoratge	L5 - 100%

OBSERVACIONS: OBS06, OBS07

COMENTARIS: Nagios, l'IDS, tallafocs i Active Directory amb la seva gestió d'usuaris proporcionen diferents capes de seguretat a l'hora d'accedir als serveis de xarxa oferts per l'organització. Tots aquests elements propocionen suficients registers per portar un control del nombre d'incidències generades en un període determinat de temps.

10.10.3 Protecció de les traces i registres	L3 - 90%

NO CONFORMITATS MENORS: NC14.

COMENTARIS: Es disposa d'una gestió poc centralitzada, cosa que en complica la seva protecció. Tot i així, en principi, tot i que de manera massa distribuïda, s'observa que estan correctament protegits i amb els permisos pertinents.

10.10.4 Traces d'administració i operació	L3 - 90%

NO CONFORMITATS MENORS: NC14.

COMENTARIS: Gestió poc centralitzada, ja que cada sistema emmagatzema les seves pròpies i això en complica l'administració i revisió necessàries.

10.10.5 Registre de fallades	L2 - 50%

NO CONFORMITATS MENORS: NC14.

COMENTARIS: Gestió poc centralitzada, ja que cada sistema emmagatzema les seves.

10.10.6 Sincronització de rellotges	L3 - 90%

NO CONFORMITATS MENORS: NC13.

COMENTARIS: La sincronització està disponible per servidors i estacions de treball, però certes càmeres IP i les màquiens de control horari presenten certes diferències respecte l'hora de la resta de sistemes sincronitzats. Cal revisar aquests sistemes, ja que en els dos casos l'hora correcta és essencial per l'execució de les seves funcions.

11. CONTROL D'ACCÉS	**67,41%**
11.1 Requisits de negoci pel control d'accés	**50,00%**
11.1.1 Política de control d'accés	L2 - 50%

NO CONFORMITATS MAJORS: NC01.

COMENTARIS: Degut a la inexistència d'una poítica de seguretat completa i ben documentada, la política de control d'accés existeix '*de facte*', però no formalment.

11.2 Gestió d'accés dels usuaris	**61,25%**
11.2.1 Registre d'usuaris	L2 - 50%

NO CONFORMITATS MAJORS: NC15.

COMENTARIS: Existeix un procediment de comunicació de baixes i altes de personal al Departament TIC. De totes maneres, no està documentat i són diversos sistemes on cal donar d'alta o de baixa l'usuari. Durant l'auditoria s'han

detectat alguns usuaris que no haurien d'existir, per tant el procediment no està funcionant correctament i cal realitzar una depuració.

11.2.2 Gestió de privilegis	L4 - 95%

OBSERVACIONS: OBS06

COMENTARIS: L'Ajuntament gestiona els privilegis dels diferents usuaris mitjançant els usuaris i grups d'Active Directory.

11.2.3 Gestió de contrasenyes d'usuari	L3 - 90%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Algunes contrasenyes no estan configurades amb una seguretat suficient per a evitar possibles atacs per aconseguir accés no autoritzat, ja que són massa obvies o algunes inclús estan apuntades en llocs visibles.

11.2.4 Revisió dels drets d'accés d'usuari	L1 - 10%

NO CONFORMITATS MAJORS: NC15.

COMENTARIS: No existeix cap procés de revisió dels drets d'accés. Tal i com s'ha vist al punt 11.2.1, s'han detectat usuaris donats d'alta que amb un procés de revisió periòdic s'haguessin detectat i eliminat.

11.3 Responsabilitat dels usuaris	**50,00%**
11.3.1 Ús de credencials	L2 - 50%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Algunes polítiques d'Active Directory respecte els temps de finalització de sessió, sessions bloquejades per temps d'inactivitat i altres directives similars no estan actives.

11.3.2 Equips d'usuaris desatesos	L3 - 90%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Algunes polítiques d'Active Directory respecte els temps de finalització de sessió, sessions bloquejades per temps d'inactivitat i altres

directives similars no estan actives.

11.3.3 Política de taules i pantalles netes	L1 - 10%

NO CONFORMITATS MAJORS: NC17.

COMENTARIS: No existeix cap procediment formal per mantenir les taules i pantalles netes. Tot i així el personal mira de portar-ho a terme dins les seves possibilitats.

11.4 Control d'accés a la xarxa	**96,43%**
11.4.1 Política d'ús dels serveis de la xarxa	L4 - 95%

OBSERVACIONS: OBS03

COMENTARIS: En l'alta del treballador, se li propociona un document on s'hi observen algunes característiques de la política d'ús dels equips informàtics. Es bastant completa. Caldria afegir algun detall però en general està bé.

11.4.2 Autenticació d'usuaris per a connexions remotes	L5 - 100%

OBSERVACIONS: OBS06, OBS07

COMENTARIS: L'autenticació d'usuaris ve suportada pel mateix Active Directory, que permet connexions remotes. En el cas de proveïdors externs, aquestes connexions estan habilitades per poder donar suport i resoldre incidències, però sempre estan actives només per un determinat nombre d'IPs d'origen, configurades en el tallafocs.

11.4.3 Autenticació de nodes a la xarxa	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: L'Ajuntament gestiona els comptes de les diferents estacions de treball permeses mitjançant Active Directory.

11.4.4 Protecció dels ports de diagnòstic i configuració remots	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: La protecció i la segregació de xarxes ve donada per l'existència

de routers i tallafocs, els quals estan confgurats correctament per l'execució de les seves funcions.

11.4.5 Segregació de les xarxes	L5 - 100%

OBSERVACIONS: OBS07

COMENTARIS: La protecció i la segregació de xarxes ve donada per l'existència de routers i tallafocs, els quals estan confgurats correctament per l'execució de les seves funcions.

11.4.6 Control de la connexió a la xarxa	L3 - 90%

NO CONFORMITATS MENORS: NC18.

COMENTARIS: En general les diferents connexions disponibles cal configurar-les per poder connectar a la xarxa corporativa. Tot i així, és possible que alguna màquina externa pugui connectar puntualment en algun lloc on està configurada. No podrà accedir a la major part dels serveis de la xarxa, però alguns si que són accessibles, tot i que tenen una importància menor. Disposaria d'accés a Internet.

11.4.7 Control d'encaminament a la xarxa	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: La protecció i la segregació de xarxes ve donada per l'existència de routers i tallafocs, els quals estan confgurats correctament per l'execució de les seves funcions.

11.5 Control d'accés al sistema operatiu	**66,67%**
11.5.1 Procediments de connexió	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: L'Ajuntament gestiona els comptes de les diferents estacions de treball permeses mitjançant un Domini i Active Directory, que disposa de DHCP i DNS. El primer cop necessita de permisos d'administració per poder intergrar-se dins la xarxa corporativa.

11.5.2 Identificació i autenticació d'usuaris	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: L'Ajuntament gestiona els comptes de les diferents estacions de treball permeses mitjançant un Domini i Active Directory, que disposa de gestió d'usuaris i grups per poder assignar diferents rols.

11.5.3 Sistema de gestió de contrasenyes	L1 - 10%

NO CONFORMITATS MAJORS: NC16.

COMENTARIS: Algunes polítiques d'Active Directory respecte el canvi periòdic de contrasenyes o l'establiment de contrasenyes complexes o no repetides no està habilitada.

11.5.4 Ús dels serveis del sistema	L3 - 90%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: L'ús detectat dels sistemes per part dels usuaris és correcte, però certs elements com l'accés automàtic a unitats externes poden portar problemes. Caldria adaptar certes polítiques d'Active Directory. Els usuaris connecten amb usuaris assignats, els quals tenen permisos limitats respecte els diferents sistemes amb els que interactuen.

11.5.5 Desconnexió automàtica de sessió	L2 - 50%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Algunes polítiques d'Active Directory respecte els temps de finalització de sessió, sessions bloquejades per temps d'inactivitat i altres directives similars no estan actives.

11.5.6 Limitació del temps de connexió	L3 - 90%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Algunes polítiques d'Active Directory respecte els temps de finalització de sessió, sessions bloquejades per temps d'inactivitat i altres directives similars no estan actives.

11.6 Control d'accés a la informació i a les aplicacions	**97,50%**
11.6.1 Restricció d'accés a la informació	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: L'Ajuntament gestiona els comptes de les diferents estacions de treball permeses mitjançant Active Directory. Les diferents aplicacions també utilitzen sistemes d'usuris, grups i rols per tal d'assignar diferents nivells d'accés a la informació, segons les necessitats dels diferents departaments.

11.6.2 Aïllament de sistemes sensibles	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: Mitjançant el tallafocs es disposa d'una zona desmilitaritzada per poder allotjar diferents sistemes que són més sensibles, ja que han de ser accedits per serveis externs.

11.7 Informàtica mòbil i teletreball	**50%**
11.7.1 Informàtica mòbil i comunicacions	L2 - 50%

NO CONFORMITATS MENORS: NC19.

COMENTARIS: Falta definir exactament una política d'ús els equips d'informàtica mòbil de l'organització. Ara mateix es funciona mitjançant recomanacions del departament de tecnologies de la informació i la comunicació.

11.7.2 Teletreball	N/A

NO APLICA.

12. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE SISTEMES D'INFORMACIÓ	**86,75%**
12.1 Requisits de seguretat en sistemes d'informació	**90,00%**
12.1.1 Anàlisi i especificació de requisits	L3 - 90%

NO CONFORMITATS MENORS: NC20.

COMENTARIS: Per desenvolupaments externs no s'observa cap problema perquè

sempre es fa un anàlisi i especificació de requisits que formen part de les condicions tècniques dels diferents concursos, contractes i/o convenis que es puguin realitzar.

12.2 Control de processos en aplicacions	**75,00%**
12.2.1 Validació de dades d'entrada	L4 - 95%

OBSERVACIONS: OBS08

COMENTARIS: Durant el desenvolupament de les aplicacions internes, sempre es mira de validar les possibles dades d'entrada de cara a evitar possibles errors o vulnerabilitats. En cas d'aplicacions web es passa per OWASP (*Open Web Application Security Project*).

12.2.2 Control de processos interns	L2 - 50%

NO CONFORMITATS MENORS: NC21.

COMENTARIS: Els processos interns de les aplicacions no sempre està ben documentat. Per tant, el manteniment de certes aplicacions es fa molt complicat si no s'hi treballa de manera continuada.

12.2.3 Integritat de missatges	L5 - 100%

OBSERVACIONS: OBS08

COMENTARIS: Es controla quan es genera programari que requereixi comunicació externa cap altres orgranitzacions o entre diferents aplicacions internes.

12.2.4 Validació de dades de sortida	L4 - 95%

OBSERVACIONS: OBS08

COMENTARIS: Sempre que es possible s'utilitza xifratge, sobretot en utilització de serveis des de l'exterior.

12.3 Controls criptogràfics	**92,50%**
12.3.1 Política d'ús de controls criptogràfics	L3 - 90%

NO CONFORMITATS MENORS: NC22.

COMENTARIS: Els controls criptogràfics que s'utilitzen en l'organització no venen determinats per cap política escrita, però si que el departament de tecnologies de la informació i la comunicació els determina en els diferents plecs tècnics en cas de definir projectes externs. Obté un nivell de compliment L3 (90%).

12.3.2 Xifratge	L4 - 95%

OBSERVACIONS: OBS08

COMENTARIS: Sempre que es possible s'utilitza xifratge, sobretot en utilització de serveis des de l'exterior. Es mira d'utilitzar protocols criptogràfics sempre que és possible en els diferents sistemes. El problema que s'observa és que alguns sistemes antics presenten complicacions en la utilització de protocols segurs ja que utilitzen versions vulnerables

12.4 Seguretat dels fitxers de sistema	**95,00%**
12.4.1 Control de programari en producció	L5 - 100%

OBSERVACIONS: OBS06

COMENTARIS: Els desenvolupaments en Linux només són accessibles per usuaris administradors (usuari *root*), mentre que en Windows disposen dels permissos necessaris per a que només siguin accessibles per l'Administrador del domini o el seu grup (definit dins *Active Directory*). No s'observen accessos no autoritzats.

12.4.2 Protecció de dades de prova	L4 - 95%

OBSERVACIONS: OBS07

COMENTARIS: La unitat robòtica de cinta realitza còpies dels diferents desenvolupaments, ja siguin en producció o no, dels diferents sistemes on es troben, tant Windows Server com Linux.

12.4.3 Control d'accés al codi font	L3 - 90%

NO CONFORMITATS MENORS: NC16.

COMENTARIS: Ve determinat per les polítiques d'accés que s'apliquen en els difrents recursos. S'ha detectat que existeix un procediment que estableix els permisos, però cal que estigui més definit i revisat, perquè s'accedeix a mode lectura algun codi de programari propi.

12.5 Seguretat en el desenvolupament i en el suport	**78,00%**
12.5.1 Procediments de control de canvis	L1 - 10%

NO CONFORMITATS MENORS: NC20.

COMENTARIS: No es disposa de cap procediment de control de canvis per les aplicacions desenvolupades internament. Caldria utilitzar-ne un com per exemple GIT o algun sistema de similars característiques.

12.5.2 Revisió tècnica de canvis en el sistema operatiu	L5 - 100%

NO CONFORMITATS MENORS: NC23.

COMENTARIS: Sempre es realitza una revisió abans i després d'aplicar canvis en els sistemes operatius, generalment actualtizacions.

12.5.3 Restricció de canvis en paquets de programari	L3 - 90%

NO CONFORMITATS MENORS: NC23.

COMENTARIS: Sempre es realitza una revisió abans i després d'aplicar canvis en el programari instal·lat. Cal tenir permissos d'administració per tal de fer-los. Molts cops es realitza còpies de seguretat segons el nivell dels canvis a realitzar, però tot i així, no exisiteix cap procediment documentat per fer aquestes còpies ni canvis segons el programari (heterogeni).

12.5.4 Fuites d'informació a través del codi	L4 - 95%

OBSERVACIONS: OBS08

COMENTARIS: Durant el desenvolupament de les aplicacions internes, sempre es mira de validar les possibles dades d'entrada de cara a evitar possibles errors o vulnerabilitats.

12.5.5 Externalització de desenvolupament de programari	L4 - 95%

OBSERVACIONS: OBS01

COMENTARIS: El fet de ser una administració local, es permet l'externalització del desenvolupament de programari. Es realitza segons la legislació vigent, on es fa per adjudicació directa, invitacions o concurs públic segons l'import del projecte a desenvolupar. En l'oferta es defineixen sempre els criteris tècnics i administratius que haurà de complir el projecte.

12.6 Gestió de les vulnerabilitats tècniques	**90,00%**
12.6.1 Control de les vulnerabilitats tècniques	L3 - 90%

NO CONFORMITATS MENORS: NC24.

COMENTARIS: Es realitzen alguns test externs per part del CESICAT, a més d'alguns anàlisi interns. Els dos resultats s'analitzen i es prenen mesures dins les possibilitats, però no se'n emmagatzema cap registre per fer-ne el seguiment al llarg del temps, cosa que n'impossibilita el seu control.

13. GESTIÓ D'INCIDÈNCIES DE SEGURETAT DE LA INFORMACIÓ	**56,67%**
13.1 Notificació d'incidències i debilitats *	**90,00%**
13.1.1 Notificació d'esdeveniments de seguretat	L3 - 90%

NO CONFORMITATS MENORS: NC25.

COMENTARIS: Està mitjanament implementada gràcies al Nagios, però això només afecta una part de les notificacions. Les entrades per part dels usuaris no s'anoten a una aplicació existent per tal de gestionar les notificacions i fer el seguiment de les incidències és poc menys que impossible. Cal millorar aquest últim punt.

13.1.2 Notificació de debilitats	L3 - 90%

NO CONFORMITATS MENORS: NC25.

COMENTARIS: Està mitjanament implementada gràcies al IDS i a l'antivirus, però resten alguns serveis que no es validen correctament. Caldria millorar el procediment.

13.2 Gestió d'incidències i millora *	**23,33%**

13.2.1 Identificació de responsabilitats i procediments	L2 - 50%

NO CONFORMITATS MAJORS: NC26.

COMENTARIS: Les responsabilitats i procediments estan parcialment definits, però no documentats i en cas d'absència pot ser problemàtic per aquesta falta de documentació dels procediments.

13.2.2 Avaluació d'incidències	L1 - 10%

NO CONFORMITATS MAJORS: NC26.

COMENTARIS: No existeixen procediments per l'avaluació de les incidències, més enllà de la improvització. Si s'utilitzés el gestor d'incidències, es podrien entrar els diferents comentaris o actuacions com a procediments per a resoldre tipus d'incidències concretes, però actualment no està sent massa utilitzat.

13.2.3 Recol·lecció d'evidències	L1 - 10%

NO CONFORMITATS MAJORS: NC26.

COMENTARIS: No existeixen procediments per la recol·lecció de les evidències, més enllà de la improvització segons el cas que s'està tractant.

14. GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI *	**42,00%**
14.1 Gestió de la continuïtat del negoci	**42,00%**
14.1.1 Procés de gestió de la continuïtat del negoci	L2 - 50%

NO CONFORMITATS MENORS: NC27.

COMENTARIS: Es realitzen certes actuacions per provar de gestionar la continuïtat del negoci, però falta més documentació per a que en quedi constància dels progressos i dels resultats de possibles proves.

14.1.2 Continuïtat de negoci i anàlisi d'impacte	L2 - 50%

NO CONFORMITATS MENORS: NC27.

COMENTARIS: Es realitza de manera informal, sense documentació ni seguint cap procediment. A més, molts cops l'anàlisi d'impacte no es redacta ni es calcula.

14.1.3 Documentació i implantació del pla de continuïtat	L1 - 10%

NO CONFORMITATS MENORS: NC27.
COMENTARIS: Pràcticament inexistent la documentació, la implantació si que es realitza en certs àmbits, però sempre de manera parcial.

14.1.4 Marc de planificació	L2 - 50%

NO CONFORMITATS MENORS: NC27.
COMENTARIS: La planificació es realitza, però no de manera global sinó independentment segons l'àmbit en que s'està actuant. Això pot comportar problemes de sincronització.

14.1.5 Procés, manteniment i avaluació de Plans de continuïtat	L2 - 50%

NO CONFORMITATS MENORS: NC27.
COMENTARIS: Es realitzen validacions del que s'ha anat realitzant i es mira cap endavant quins projectes cal anar realitant, però sempre a molt curt termini i sense aportar massa documentació ni relació entre els diferents projectes.

15. CONFORMITAT	**31,94%**
15.1 Conformitat amb requisits legals	**95,83%**
15.1.1 Identificació de la legislació aplicable	L5 - 100%

OBSERVACIONS: OBS01
COMENTARIS: El fet de ser una administració local implica identificar i complir les diferents lleis aplicables. El departament de Secretaria i el d'Intervenció vetllen per a que això sigui així.

15.1.2 Dret de la propietat intel·lectual *	L5 - 100%

OBSERVACIONS: OBS01
COMENTARIS: El fet de ser una administració local implica identificar i complir les diferents lleis aplicables, entre elles les del dret de la propietat intel·lectual. Control necessari per certificació de la ISO 27001:2005.

L'auditoria no ha mostrar programari sense llicència vàlida.

15.1.3 Control de seguretat de registres de l'organització *	L3 - 90%

NO CONFORMITATS MENORS: NC28.

COMENTARIS: Es realitza còpia de certs registres, però s'ha observat durant el procés d'auditoria que alguns sistemes no en tenen configurada cap còpia, de manera que aquests registres poden perder-se o modificar-se i no es podrien recuperar.

15.1.4 Protecció dades de caràcter personal i de la intimitat *	L5 - 100%

OBSERVACIONS: OBS01

COMENTARIS: El fet de ser una administració local implica identificar i complir les diferents lleis aplicables. Control necessari per certificació de la ISO 27001:2005. En aquest cas s'està realitzant correctament tal i com es defineix a la Llei Orgànica de Protecció de dades.

15.1.5 Evitar mal ús de recursos de tractament de la informació	L3 - 90%

NO CONFORMITATS MENORS: NC29.

COMENTARIS: De tant en tant es detecten incidències provocades per mal ùs de recursos de tractament de la informació. Això és degut a una falta de formació per part del personal, ja no de seguretat sinó d'aplicacions o processos concrets.

15.1.6 Reglamentació de controls de xifratge	L4 - 95%

OBSERVACIONS: OBS01

COMENTARIS: El fet de ser una administració local implica identificar i complir les diferents lleis aplicables.

15.2 Compliment del marc normatiu	0,00%
15.2.1 Compliment de polítiques i normes	L0 - 0%

NO CONFORMITATS MAJORS: NC30.

COMENTARIS: No es realitza actualment cap verificació formal de les diferents polítiques (actualment insuficients) i normes que afecten l'organització en els aspectes tecnològics i de tractament de dades.	
15.2.2 Comprovació de la conformitat tècnica	L0 - 0%
NO CONFORMITATS MAJORS: NC30. **COMENTARIS:** Actualment no s'està realitzant, ni tampoc existeixen registres per poder informar dels resultats de les diferents comprovacions que es realitzin.	
15.3 Auditoria de sistemes	**0,00%**
15.3.1 Controls d'auditoria de sistemes	L0 - 0%
NO CONFORMITATS MAJORS: NC03. **COMENTARIS:** No es realitzen ni es planifiquen auditories de cap tipus.	
15.3.2 Protecció d'eines d'auditoria	L0 - 0%
NO CONFORMITATS MAJORS: NC03. **COMENTARIS:** No existeixen actualment eines d'auditoria internes, tot i que són necessàries per poder-les executar correctament.	

Taula 8-1: Taula resum de l'auditoria de compliment

8.3 NO CONFORMITATS

A continuació es mostren les diferents no conformitats que s'han anat informant durant l'auditoria de compliment, omplint les respectives fitxes (el model de les quals es pot consultar en l'Annex III del present document, apartat A3.1). S'han obviat els camps innecessaris al tractar-se d'un resum, com són la resolució, les signatures i resposanbilitats, així com les diferents dates.

NO CONFORMITAT:	**NC01**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	

La política de seguretat de l'organització és incompleta, manca molta informació i no existeix un procés de revisió per tal de poder-la anar adaptant a les possibles necessitats o modificacions de l'organització. Altres documents del SGSI també estan incomplets o no existeixen.	
PARÀGRAF DE LA NORMA:	**5.1.1** Document de política de seguretat **5.1.2** Revisió de la política de seguretat **6.1.1** Comitè de Seguretat **6.1.2** Coordinació **11.1.1** Política de control d'accés
DOCUMENT SGSI:	Política de Seguretat i altres documents del SGSI.
ACCIÓ CORRECTORA PROPOSADA:	
- **PROJECTE PROJ-003** - Modificació de la Política completant-la amb la informació addicional necessàira. - Creació d'un procés de revisió de la política, d'execució periòdica.	

Taula 8-2: No conformitat NC01

NO CONFORMITAT:	**NC02**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Existeix una certa manca d'informació al respecte d'algunes de les funcions dels diferents departaments o càrrecs. Es precisa la documentació d'aquestes funcions.	
PARÀGRAF DE LA NORMA:	**6.1.3** Assignació de responsabilitats **10.1.3** Segregació de funcions
DOCUMENT SGSI:	Política de Seguretat - Rols i responsabilitats
ACCIÓ CORRECTORA PROPOSADA:	
- Generar documentació per determinar les funcions exactes dels diferents càrrecs i departaments per evitar conflictes o solapacions entre el personal.	

Taula 8-3: No conformitat NC02

NO CONFORMITAT:	**NC03**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No s'ha contractat mai cap empresa o servei extern per tal de realtizar una auditoria. Tampoc existeix cap procediment per tal de realitzar-les de manera periòdica.	
PARÀGRAF DE LA NORMA:	**6.1.8** Revisió independent de la seguretat de la informació **15.3.1** Controls d'auditoria de sistemes

	15.3.2 Protecció d'eines d'auditoria
DOCUMENT SGSI:	Auditories externes. Registres d'auditoria.
ACCIÓ CORRECTORA PROPOSADA:	
- Introduir al pressupost partida necessària per execució d'auditories i estudies externs un cop implantats els diferents projectes. - Implantació del **PROJ-011**.	

Taula 8-4: No conformitat NC03

NO CONFORMITAT:	**NC04**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Tot i que en contractes o convenis amb tercers existeixen certes clàusules relatives a aspectes de seguretat de la informació i confidencialitat, caldria revisar les d'alguns contractes o convenis, ja que són insuficients en determinats casos, o deixen algun aspecte obert.	
PARÀGRAF DE LA NORMA:	**6.2.1, 6.2.2, 6.2.3**
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Revisió d'alguns contractes i convenis per tenir-ho en compte en futures renovacions o contractacions per part del Departament de Secretaria.	

Taula 8-5: No conformitat NC04

NO CONFORMITAT:	**NC05**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No conformitat relacionada amb el manteniment de l'inventari d'actius de l'organització. Existeix, però no s'actualitza periòdicament ni es manté de manera eficient. A més, cert persnoal no utilitza correctament algun actiu de l'organització. Entre aquests usos incorrectes es troba el marcatge i classificació de certs actius d'informació, i conceptes de seguretat.	
PARÀGRAF DE LA NORMA:	**7.1.1, 7.1.3, 7.1.5, 8.2.2**
DOCUMENT SGSI:	Inventari d'actius. Formació del personal.
ACCIÓ CORRECTORA PROPOSADA:	
- Execució del projecte **PROJ-004**. - Formació del personal en projecte **PROJ-007**.	

Taula 8-6: No conformitat NC05

NO CONFORMITAT:	**NC06**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Definició de rols i responsabilitats, termes i condicions de relació laboral i supervisió d'obligacions definides però no es disposen de valors de sortida registrats per poder identificar si els processos estan millorant o no.	
PARÀGRAF DE LA NORMA:	**8.1.1, 8.1.3, 8.2.1**
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Implementació del projecte **PROJ-006**.	

Taula 8-7: No conformitat NC06

NO CONFORMITAT:	**NC07**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Algunes seus o dependències han patit robatoris menors de poca importància, però les conseqüències podrien haver estat més greus.	
PARÀGRAF DE LA NORMA:	**9.1.1** Perímetre de seguretat física
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Realitzar actuacions necessàries entre Oficina Tècnica municipal i Policia Municipal per tal de modificar físicament alguna de les seus per evitar possibles robatoris.	

Taula 8-8: No conformitat NC07

NO CONFORMITAT:	**NC08**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Existeixen controls d'incendis i fums, així com extintors en totes les seus de l'Ajuntament. De totes maneres, s'ha detectat que no existeixen controls de temperatura i humitat en els Centres de processament de dades, els quals disposen d'aire acondicionat (en alguns punts, insuficient per la quantitat de calor generada).	

PARÀGRAF DE LA NORMA:	**9.1.4** Protecció contra amenaces internes i externes
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Instal·lació i configuració d'alertes per control de temperatura i humitat als CPD. - Execució del Projecte **PROJ-005** (Millora de climatització en CPD).	

Taula 8-9: No conformitat NC08

NO CONFORMITAT:	**NC09**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No es disposa d'un procediment per sol·licitar l'autorització de sortida d'actius de l'organització. La seguretat fora dels locals queda exposada, més per falta de formació dels empleats respecte la seguretat de la informació. És a dir, qualsevol pot accedir a la informació d'un portàtil perdut o robat, però si la informació està correctament xifrada l'impacte és mínim.	
PARÀGRAF DE LA NORMA:	**9.2.5** Seguretat fora dels locals **9.2.7** Autorització de sortida **10.7.1** Gestió de suports extraïbles **10.8.3** Suports físics en trànsit
DOCUMENT SGSI:	Registres de formació. Manuals o procediments de xifratge.
ACCIÓ CORRECTORA PROPOSADA:	
- Execució del **PROJ-007**, formació del personal en matèria de seguretat de les TIC.	

Taula 8-10: No conformitat NC09

NO CONFORMITAT:	**NC10**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
El manteniment dels equips és bastant correcte, però existeixen diversos problemes detectats, com són alguns sistemes no actualitzats correctament (degut a infecció de codi maliciós o sistema anticuat).	
PARÀGRAF DE LA NORMA:	**9.2.4** Manteniment dels equips **10.4.1** Protecció contra codi maliciós **10.4.2** Protecció contra codi descarregat en el client
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	

- Execució del **PROJ-001**, adquisició del antivirus. - Control d'actualitzacions de sistema. - Canvi de sistemes antics ja no soportats i que no reben ni suport ni actualitzacions de seguretat en cas de ser programari.

Taula 8-11: No conformitat NC10

NO CONFORMITAT:	**NC11**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
L'organització pràcticament no disposa de procediments formalment documentats i/o aplicats. Entre alters, tampoc disposa d'una gestió de canvis apropiada.	
PARÀGRAF DE LA NORMA:	**10.1.1** Documentació de procediments **10.1.1** Gestió de canvis **10.7.3** Procediments d'utilització de la informació **10.8.1** Polítiques i procediments d'intercanvi d'informació
DOCUMENT SGSI:	Documentació de procediments.
ACCIÓ CORRECTORA PROPOSADA:	
- Execució dels projectes **PROJ-001 i PROJ-011**.	

Taula 8-12: No conformitat NC11

NO CONFORMITAT:	**NC12**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
L'organització pràcticament no disposa de procediments formalment documentats i/o aplicats. Entre alters, tampoc disposa d'una gestió de canvis apropiada.	
PARÀGRAF DE LA NORMA:	**10.2.3** Gestió de canvis en els serveis
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Amb més personal és probable que aquesta gestió de canvis sigui més àgil, per tant, caldria executar el projecte **PROJ-013**.	

Taula 8-13: No conformitat NC12

NO CONFORMITAT:	**NC13**

TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
La sincronització dels rellotges en algun sistema no és l'òptim, donat que cal fer-lo manualment (màquines de control horari) o càmeres IP i alguns telèfons IP. D'altra banda, la major part dels ordinadors i servidors utilitzen NTP per sincronitzar l'hora de manera automàtica.	
PARÀGRAF DE LA NORMA:	**10.10.6** Sincronització de rellotges
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Configuració de possible servei NTP (intern o extern) o creació i implantació de procediment periòdic d'actualització d'hora en sistemes que no admetin NTP.	

Taula 8-14: No conformitat NC13

NO CONFORMITAT:	NC14
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Els diferents registres i traces recollides pels diferents sistemes es troben en general dins el mateix sistema, de manera que en fa més complexa la seva gestió i interpretació. La implantació de controls i la seva validació periòdica es fa més difícil i poden aportar dades incorrectes.	
PARÀGRAF DE LA NORMA:	**10.10.1** Registre d'activitats **10.10.3** Protecció de traces i registres **10.10.4** Traces d'administració i operació **10.10.5** Registre de fallades
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Centralització dels diferents registres i incidències dels diferents sistemes per facilitar-ne el tractament i interpretació.	

Taula 8-15: No conformitat NC14

NO CONFORMITAT:	NC15
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Alguns procediments (no documentats) entre el Departament de Recursos Humans i el Departament TIC no estan funcionant correctament, ja que s'han trobat certs usuaris en el sistema de treballadors antics de la casa.	

PARÀGRAF DE LA NORMA:	**11.2.1** Registre d'usuaris **11.2.4** Revisió dels drets d'accés
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Execució de projecte **PROJ-006** per depuració de procediments relacionats amb departament de Recursos Humans i Departament TIC. - Creació de procediment per revisar els drets d'accés periòdicament.	

Taula 8-16: No conformitat NC15

NO CONFORMITAT:	**NC16**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Algunes de les polítiques d'Active no estan ben aplicades o configurades per tal de limitar certs aspectes de les estacions de treball, com per exemple: contrasenyes més complexes, política de canvi de contrasenya obligada, etc.	
PARÀGRAF DE LA NORMA:	**11.2.3** Gestió de contrasenyes **11.3.2** Equips d'usuaris desatesos **11.5.3** Sistema de gestió de contrasenyes **11.5.5** Desconnexió automàtica de sessió **11.5.6** Limitació del temps de connexió **12.4.3** Control d'accés al codi font
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Execució de projecte **PROJ-012** per crear prodeciment de revisió de polítiques d'Active Directory, i modificació de les actuals per millorar certs aspectes.	

Taula 8-17: No conformitat NC16

NO CONFORMITAT:	**NC17**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No existeix cap política de taules i pantalles netes de manera formal. Per tant, al no estar definida es deixa a la bona voluntat del treballador, quan realment es tracta d'un punt important a tenir en compte de cara la confidencialitat de les dades que es tracten en els diferents departaments. Cal definir-ho formalment i dotar de formació al personal per realitzar una tasca de conscienciació.	
PARÀGRAF DE LA NORMA:	**11.3.3** Política de taules i pantalles netes

DOCUMENT SGSI:	Polítiques d'accés a xarxa.
ACCIÓ CORRECTORA PROPOSADA:	
- Execució del projecte **PROJ-001**, i formació del personal amb el **PROJ-007**.	

Taula 8-18: No conformitat NC17

NO CONFORMITAT:	**NC18**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
El control d'accés a la xarxa no és perfecte. Hi ha certs punts de connexió poc vigilats on qualsevol que connecti un ordinador pot accedir a la xarxa corporativa. L'accés permet connexió a Internet i visualitzar algun servei que és de poca importància.	
PARÀGRAF DE LA NORMA:	**11.4.6** Control de la connexió a la xarxa
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Configuració per defecte de ports no utilitzats per estacions de treball de manera que no permetin cap tipus de connexió. Configurar-los només en cas de necessitat i de manera temporal.	

Taula 8-19: No conformitat NC18

NO CONFORMITAT:	**NC19**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No existeixen polítiques d'ús dels diferents dispositius mòbils corporatius (PDAs, portàtils i Smartphones). Tot i així se segueixen certes bones pràctiques que recomana el departament de tecnologies de la informació i la comunicació.	
PARÀGRAF DE LA NORMA:	**11.7.1** Informàtica mòbil
DOCUMENT SGSI:	Polítiques d'ús d'equipament tecnològic
ACCIÓ CORRECTORA PROPOSADA:	
- Definició de les polítiques d'ús dels diferents tipus de dispositius mòbils.	

Taula 8-20: No conformitat NC19

NO CONFORMITAT:	**NC20**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR

DESCRIPCIÓ DE LA NO CONFORMITAT:	
En els desenvolupaments propis, es pateix de falta de recursos econòmics i humans. Es realitzen les tasques necessàries i s'inicien nous projectes, però manca cerat documentació i procediments dins del desenvolupament de programari que no es poden assolir.	
PARÀGRAF DE LA NORMA:	**12.1.1** Anàlisi i especificació de requeriments
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- L'execució del projecte PROJ-013 reuduiria significativament la manca de recursos humans del departament, permetent assolir una millor gestió de processos en el workflow dels desemvolupaments propis.	

Taula 8-21: No conformitat NC20

NO CONFORMITAT:	**NC21**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Poca documentació en els processos interns de les aplicacions. Per tant, el manteniment de certes aplicacions es fa molt complicat si no s'hi treballa de manera continuada o si el desenvolupador no és l'autor del codi o sistema amb el que treballa.	
PARÀGRAF DE LA NORMA:	**12.2.2** Control de processos interns
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Generació de la documentació dels processos interns de les aplicacions.	

Taula 8-22: No conformitat NC21

NO CONFORMITAT:	**NC22**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No existeixen polítiques d'ús de controls criptogràfics degudament documentades i aplicades. Tot i així es tenen en compte els serveis que poden emprar criptografia per tal d'agumentar el nivell de confidencialitat de les transmissions de dades.	
PARÀGRAF DE LA NORMA:	**12.3.1** Política d'ús de controls criptogràfics
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	

- Documentar les polítiques '*de facte*' que s'estan emprant acutalment.

Taula 8-23: No conformitat NC22

NO CONFORMITAT:	**NC23**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Els canvis en el programari només els poden realitzar els administradors. A més, es realitza una revisió del sistema abans i després dels canvis, així com còpies de seguretat si n'hi ha la necessitat. Tot i així, cal destacar que caldria realitzar algun procediment escrit per actualitzacions de sistemes (periodicitat de revisions i reinicis per aplicació de canvis), així com documentar els diferents canvis en el programari i com realitzar-los (degut a que és molt heterogeni).	
PARÀGRAF DE LA NORMA:	**12.5.2** Revisió tècnica de canvis en el sistema operatiu **12.5.3** Restricció de canvis en paquets de programari
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Realitzar algun procediment escrit per actualitzacions de sistemes (periodicitat de revisions i reinicis per aplicació de canvis). - Documentar els diferents canvis en el programari i com realitzar-los.	

Taula 8-24: No conformitat NC23

NO CONFORMITAT:	**NC24**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No se emmagatzema cap registre dels diferents test de vulnerabilitats tant externs com interns per fer-ne el seguiment al llarg del temps, cosa que n'impossibilita el seu control. És a dir, es fa el test (intern o extern per part del CESICAT), s'analitzen els resultats i es realitzen diverses actuacions, però no queda constància del resultat passat el temps. Això és necessari per controlar la evolució del control al llarg del temps.	
PARÀGRAF DE LA NORMA:	**12.6.1** Control de les vulnerabilitats tècniques
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Emmagatzemar els registres dels diferents controls de les vulnerabilitats tècniques.	

Taula 8-25: No conformitat NC24

NO CONFORMITAT:	**NC25**

TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Existeix una aplicació per tal de poder gestionar les diferents incidències, així com un formulari per a que el personal pugui donar-ne d'alta de pròpies. Tot i així, aquesta aplicació no és massa utilitzada i moltes incidències queden pendents d'anotar. Això n'impossibilita el control i la gestió, de manera que cal fer més ènfasi en utilitzar aquest tipus de programari. Algunes incidències són detectades per Nagios o per l'IDS (Intrusion Detecion System), però cal agrupar els diferents resultats per analitzar-los i tenir-los en compte.	
PARÀGRAF DE LA NORMA:	**13.1.1** Notificació d'esdeveniments de seguretat **13.1.2** Notificació de debilitats
DOCUMENT SGSI:	Notificació d'incidències de seguretat / debilitats
ACCIÓ CORRECTORA PROPOSADA:	
- Utilització del programari de gestió d'incidències. - Agrupació de resultats de notificacions del Nagios amb alarmes de l'IDS.	

Taula 8-26: No conformitat NC25

NO CONFORMITAT:	**NC26**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Degut a que el programari existent per la gestió d'incidències no s'està emprant de manera general i correcta, no hi ha manera de tenir emmagatzemats els diferents procediments pels diferents tipus d'incidències. L'avaluació es realitza cada cop sense consultar cap històric, i la recol·lecció d'evidències s'improvitza segons el cas o el tipus d'incidència.	
PARÀGRAF DE LA NORMA:	**13.2.1** Identificació de responsabilitats i procediments **13.2.2** Avaluació d'incidències **13.2.3** Recol·lecció d'evidències
DOCUMENT SGSI:	Rols i responsabilitats – Gestió incidències
ACCIÓ CORRECTORA PROPOSADA:	
- Utilització del programari de gestió d'incidències i mantenir històric i solució d'aquestes incidències, així com notes al respecte de la recol·lecció d'evidències.	

Taula 8-27: No conformitat NC26

NO CONFORMITAT:	**NC27**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	

Exsiteixen importants carències generals en la gestió dels plans de continuïtat, ja sigui en la seva gestió, planificació, anàlisi d'impacte o en el seu manteniment i avaluació posterior. S'estan realitzant projectes per implementar certs plans de continuïtat, però sense una visió global sinó de manera particular i projecte per projecte. Això evita la possibilitat de realitzar controls al respecte del seu progrés i eficiència.	
PARÀGRAF DE LA NORMA:	**14.1.1** Procés de gestió de la continuïtat del negoci **14.1.2** Continuïtat de negoci i anàlisi d'impacte **14.1.4** Marc de planificació **14.1.5** Procés, manteniment i avaluació de Plans de continuïtat
DOCUMENT SGSI:	Plans de continuïtat / Anàlisi d'impacte
ACCIÓ CORRECTORA PROPOSADA:	
- Execució del **PROJ-009**, on es definiran els diferents plans de continuïtat i la seva gestió i manteniment.	

Taula 8-28: No conformitat NC27

NO CONFORMITAT:	**NC28**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Es realitza còpia de certs registres, però s'ha observat durant el procés d'auditoria que alguns sistemes no en tenen configurada cap còpia, de manera que aquests registres poden perder-se o modificar-se i no es podrien recuperar en cas de necessitat. Entre aquests sistemes destaquen l'IDS, el Nagios, el servidor de correu i el tallafocs. Cal emmagatzemar correctament aquests registres de log per evitar-ne la seva pèrdua o modificació malintencionada.	
PARÀGRAF DE LA NORMA:	**15.1.3** Control de seguretat de registres de l'organització
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Configurar les còpies de seguretat per cobrir els diferents registres dels diferents sistemes, incorporant els que falten.	

Taula 8-29: No conformitat NC28

NO CONFORMITAT:	**NC29**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
Existeixen certs problemes en aplicacions i programari que els treballadors fan servir per funcionalitats del seu lloc de treball. No tant en procediments diàris, però si al realitzar tasques que realitzen molt puntualment. Això genera moltes incidències que es podrien	

solventar amb formació o una bona documentació d'aquestes aplicacions que s'utilitzen amb molt poca freqüència.	
PARÀGRAF DE LA NORMA:	**15.1.5** Evitar mal ús de recursos de tractament de la informació
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Implementar altres plans de formació, no només de seguretat, per facilitar al personal la utilització del programari necessari per desenvolupar les diferents tasques dins l'Ajuntament.	

Taula 8-30: No conformitat NC29

NO CONFORMITAT:	**NC30**
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR
DESCRIPCIÓ DE LA NO CONFORMITAT:	
No es realitza actualment cap verificació formal de les diferents polítiques (actualment insuficients) i normes que afecten l'organització en els aspectes tecnològics i de tractament de dades. Tampoc es realitza la comprovació de la conformitat tècnica.	
PARÀGRAF DE LA NORMA:	**15.2.1** Compliment de polítiques i normes **15.2.2** Comprovació de la conformitat tècnica
DOCUMENT SGSI:	N/A
ACCIÓ CORRECTORA PROPOSADA:	
- Crear els respectius procediments per realitzar la comprovació de la conformitat tècnica, així com revisar les diferents polítiques i normes.	

Taula 8-31: No conformitat NC30

8.4 OBSERVACIONS

A continuació es mostren les diferents observacions que s'han anat informant durant l'auditoria de compliment, omplint les respectives fitxes (el model de les quals es pot consultar en l'Annex III del present document, apartat A3.2).

NÚM. OBSERVACIÓ:	**OBS01**
DESCRIPCIÓ DE L'OBSERVACIÓ:	
El fet de ser una administració pública aporta certs processos relacionats amb la intervenció econòmica o aspectes legals (secretaria) que estan degudament comentats i se n'observa un funcionament del tot correcte. A més, es disposa de certs elements com són	

el registre d'entrada i sortida, així com el gestor d'expedients, que ajuden a realitzar i mantenir una documentació exhaustiva de tots els procediments interns o externs de l'Ajuntament.			
PARÀGRAF DE LA NORMA:	6.1.4, 6.1.5, 6.1.6, 6.1.7, 8.1.2, 8.2.3, 10.9.3, 10.2.1, 10.8.2, 12.5.5, 15.1.1, 15.1.2, 15.1.4	**DOCUMENT DEL SGSI:**	N/A

Taula 8-32: Observació OBS01

NÚM. OBSERVACIÓ:	**OBS02**		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
La propietat i la classificació dels actius està ben gestionada dins l'organització. Per una banda, la propietat queda sempre delimitada a un departament en concret, tot i que certs actius poden ser accedits per altres departaments. D'altra banda, els actius d'informació estan gestionats segons la seva classificació.			
PARÀGRAF DE LA NORMA:	7.1.2, 7.2.1	**DOCUMENT DEL SGSI:**	N/A

Taula 8-33: Observació OBS02

NÚM. OBSERVACIÓ:	**OBS03**		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
El departament de personal disposa de certs procediments per a gestionar les baixes i altes de personal, així com la comunicació a altres departaments de les eliminacions de drets d'accés.			
PARÀGRAF DE LA NORMA:	7.1.2, 7.2.1, 11.4.1	**DOCUMENT DEL SGSI:**	N/A

Taula 8-34: Observació OBS03

NÚM. OBSERVACIÓ:	**OBS04**		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
Els diferents despatxos amb informació sensible disposen de pany amb clau per evitar accessos no autoritzats. De la mateixa manera, els diferents CPDs també disposen d'aquest tipus de pany.			
PARÀGRAF DE LA NORMA:	9.1.2, 9.1.3	**DOCUMENT DEL SGSI:**	N/A

Taula 8-35: Observació OBS04

NÚM. OBSERVACIÓ:	OBS05		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
Els diferents equips estan ubicats en seus o despatxos amb entrades controlades durant l'horari d'atenció al client, i es tanca degudament al finalitzar la jornada (menys Policia). D'altra banda, es disposa de sistemes d'alimentació ininterrompuda per donar cobertura les sales de CPD. El cablejat sempre està cobert per canaleta o dins la paret en el cas del coure, o va soterrat en rasa (en el cas de fibra), menys en algun punt concret que va grimpat per façana. Es realitza una destrucció dels elements que poden ser susceptibles de contenir dades, així com un reciclatge correcte de tots els elements tecnològics o en paper.			
PARÀGRAF DE LA NORMA:	9.2.1, 9.2.2, 9.2.3, 9.2.6, 10.7.2	**DOCUMENT DEL SGSI:**	N/A

Taula 8-36: Observació OBS05

NÚM. OBSERVACIÓ:	OBS06		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
La xarxa de l'Ajunatment està gestionada mitjançant un controlador de Domini Windows Server 2008, el qual disposa dels serveis necessaris (*Active Directory*) per tal de gestionar els diferents permisos i accessos a serveis i/o informació disponible a nivell intern o corporatiu.			
PARÀGRAF DE LA NORMA:	10.4.2. 10.6.1, 10.6.2, 10.7.4, 10.10.2, 11.2.2, 11.4.6, 11.6.1, 11.4.2, 11.5.1, 11.5.2, 12.4.1	**DOCUMENT DEL SGSI:**	N/A

Taula 8-37: Observació OBS06

NÚM. OBSERVACIÓ:	OBS07		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
Es diposa de certs elements o serveis de xarxa per tal d'administrar-ne el seu ús correcte i la seva seguretat i monitoratge. Entre aquests elements destaquem: tallafocs, proxy, nagios (monitoratge de serveis i sistemes) amb notificacions per SMS i IDS (intrusion detection system), així com serveis de filtratge de virus i spam pel correu electrònic. Respecte la seguretat, l'Ajuntament també disposa d'una unitat robòtica de xarxa amb la qual realitzar centralitzadament les còpies de seguretat dels diferents servidors.			
PARÀGRAF DE LA	10.2.2, 10.3.1,	**DOCUMENT DEL**	N/A

NORMA:	10.4.1, 10.5.1, 10.6.1, 10.6.2, 10.10.2, 10.8.4, 10.8.5, 11.4.2, 11.4.4, 11.4.5, 11.4.7, 11.6.2, 12.4.2	**SGSI:**	

Taula 8-38: Observació OBS07

NÚM. OBSERVACIÓ:	**OBS08**		
DESCRIPCIÓ DE L'OBSERVACIÓ:			
Separació d'entorns en producció i desenvolupament. Aquest últim entorn serveix per la realització de proves de nous serveis o sistemes, o per la prova de modificacions crítiques o imporants en sistemes existents. Per cada desenvolupament es miren de revisar els diferents canvis, dades d'entrada i sortida per poder realitzar conjunts de proves i integritat dels missatges, així com possibilitat de xifratge, sobretot en comunicacions cap a l'exterior.			
PARÀGRAF DE LA NORMA:	10.1.4, 12.2.1, 12.2.3, 12.2.4, 12.3.2, 12.5.4	**DOCUMENT DEL SGSI:**	N/A

Taula 8-39: Observació OBS08

8.5 PRESENTACIÓ DE RESULTATS DE L'AUDITORIA DE COMPLIMENT

Un cop realitzada l'auditoria del compliment, en podem extreure un conjunt de dades que permetran obtenir una idea de l'estat actual de l'organització.

S'han anotat, durant l'auditoria de compliment, els següents elements:

- 30 no conformitats
  - 9 no conformitats majors
  - 21 no conformitats menors
- 8 observacions

Algunes de les no conformitats pertanyen a controls que són necessaris per poder obtenir una certificació respecte la norma ISO/IEC 27001:2005. El nivell de maduresa dels diferents controls ens permet obtenir la representació gràfica que es mostra en la *Figura 8-1*, on s'observa el percentatge de controls que es troben per cada nivell de maduresa.

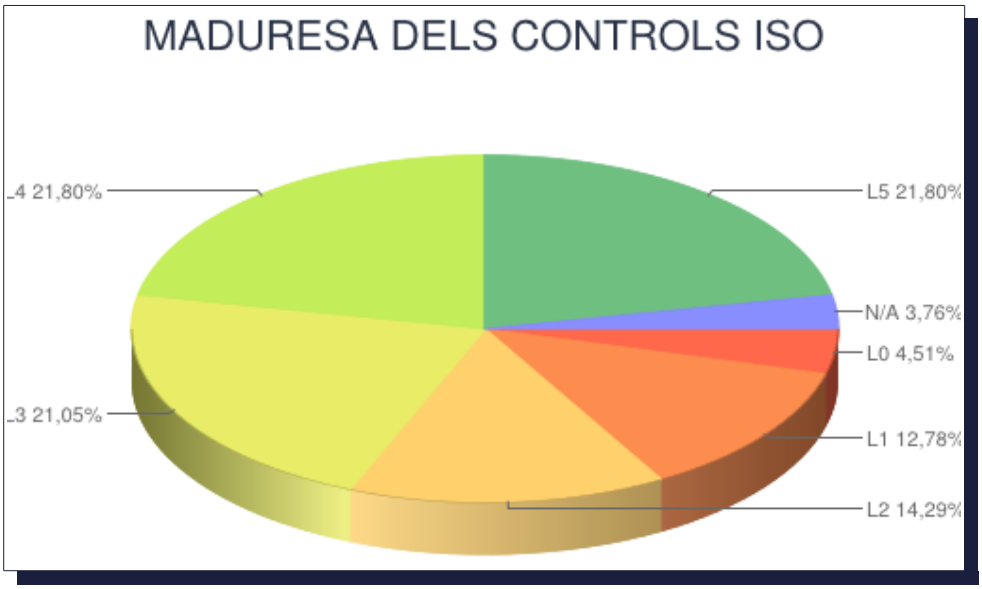

Figura 8-1: Percentatges dels nivells de maduresa dels diferents controls de la ISO 27001

Tal i com es pot observar en la *Figura 8-1*, tot i que té controls inexistents, només representen el 4,51% dels 133 totals. Ara bé, sumant-hi els nivells L1 (10%) i L2 (14,29%) ja representen un 31,58% del total. Per sobre del 90% del compliment (L3, L4 i L5) hi ha el 64,65% dels controls. Per tant, podríem afirmar que en una tercera part dels controls s'hi necessita executar alguna acció correctora o procediment per tal de millorar-ne la maduresa, si acceptem com a valor vàlid que el nivell de compliment estigui en el 90% o superior. D'altra banda, la *Figura 8-2* ens mostra un diagrama de radar amb la maduresa màxima dels diferents dominis i la maduresa actual de l'organització respecte cadascun d'ells.

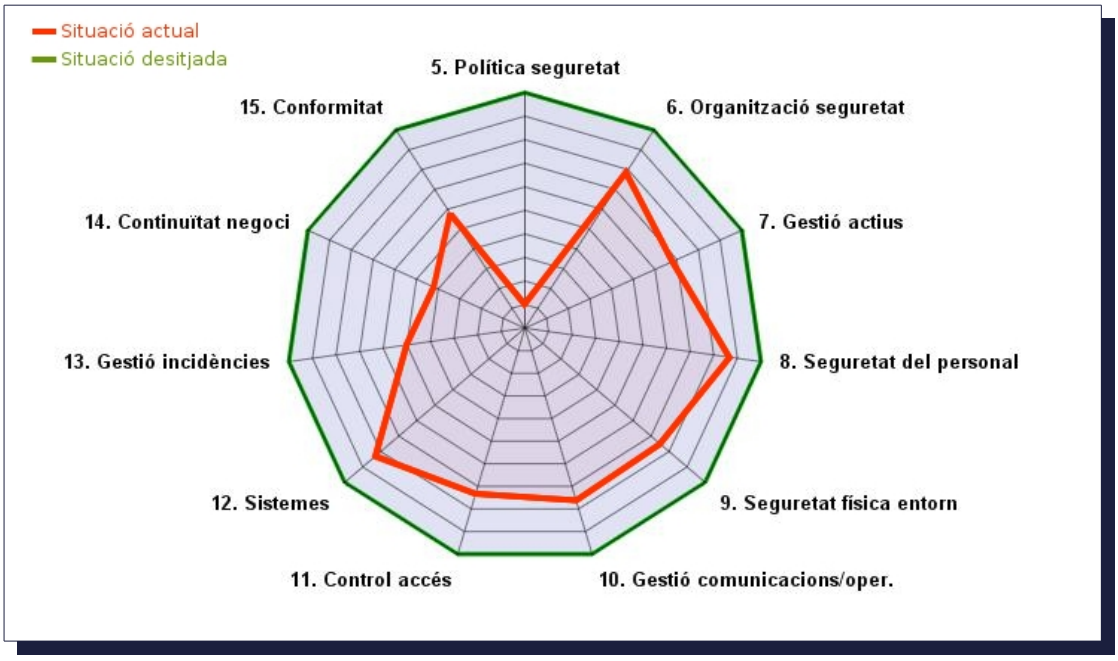

Figura 8-2: Compliment actual dels diferents dominis de la ISO 27001

El gràfic de la *Figura 8-2* permet, amb un cop d'ull, saber quins aspectes de l'organització necessiten més actuacions per tal d'adpatar-se a la ISO. En aquest cas, es pot observar com el domini 5 'Política de Seguretat', el 13 'Gestió d'incidències', el 14 'Continuitat del negoci' i el 15 'Conformitat) surten bastant mal parats.

Tot i així, si en els tres anys següents s'aconsegueixen executar i implantar correctament els projectes definits en l'apartat 7 del present document, el diagrama de radar del compliment dels dominis de la ISO passaria a ser similar al que es mostra de color groc en la *Figura 8-3*.

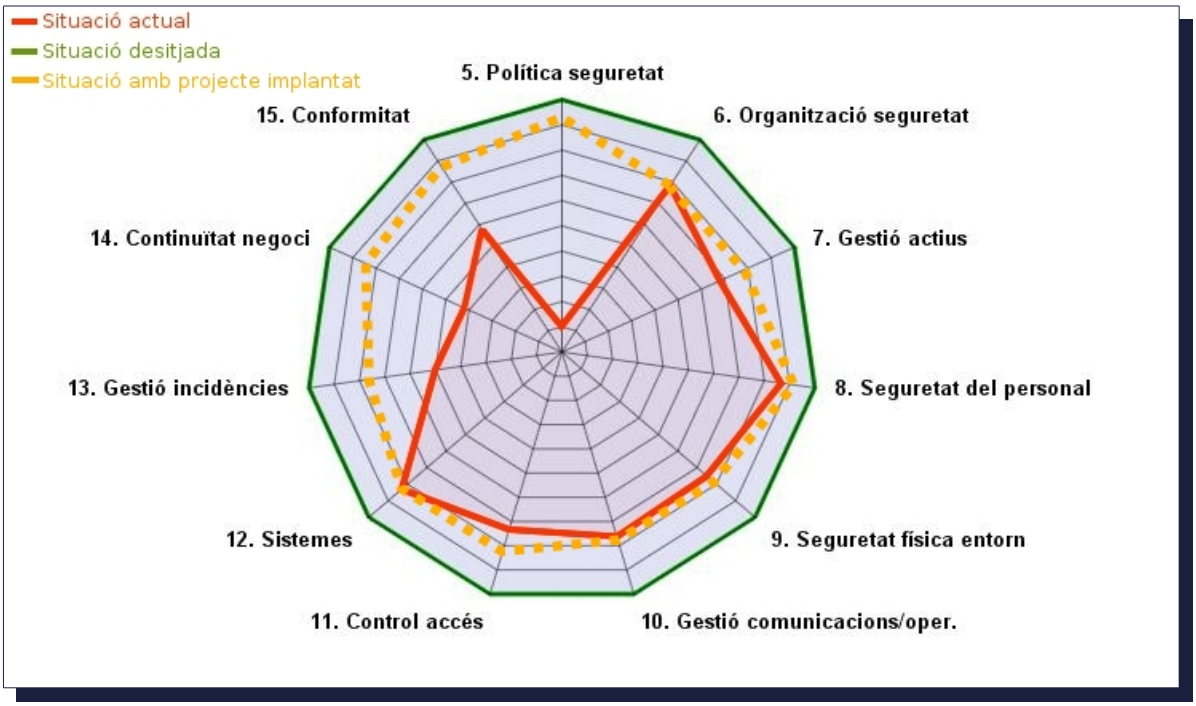

Figura 8-3: Compliment dels diferents dominis de la ISO 27001 després d'executar projectes

Tal i com es pot observar en l'anterior figura, s'aconsegueix una millora considerable dels dominis que estaven en un nivell de compliment baix, mentre que a la vegada s'augmenta el nivell de compliment de la resta de dominis de la ISO.

A1. ANNEX I – DOCUMENTS DEL SISTEMA DE GESTIÓ DOCUMENTAL

A1.1 POLÍTICA DE SEGURETAT

Resum de la Política de seguretat signat per la direcció de l'organització:

L'Ajuntament de Riberola depèn, cada dia en major mesura, dels elements vinculats a les Tecnologies de la Informació i la Comunicació per aconseguir complir els seus objectius.

La finalitat de qualsevol servei definit i portat a terme per part de l'organització és la d'oferir el millor servei possible, millorant els nostres processos i respectant els drets i les lleis vigents actualment.

Per tant, l'Ajuntament de Riberola ha desenvolupat una Política de Seguretat i els corresponents procediments relacionats amb aquesta Política, per tal de garantir la confidencialitat, l¡autenticitat, la integritat i la disponibilitat de la informació que es gestiona des dels diferents departaments de l'organització.

Mitjançant aquest document, el Govern Municipal vol deixar constància expressa del coneixement de les polítiques desenvolupades en aquest sentit, així com de la seva aprovació per part de la Junta de Govern Local en la sessió del X del XXXX (JGL XX/XXXX).

Els documents on es detalla la Política de Seguretat han de ser coneguts i assumits per part de tots els treballadors de l'organització, de manera que s'executin i es tinguin en compte com una part més de les seves tasques diàries. Són consultables mitjançant l'aplicació d'Intranet, o es pot demanar una còpia impresa al Departament de Recursos Humans.

30 d'abril del 2013, Riberola

[SIGNATURA]

Julius Henry Marx

Alcalde de l'Ajuntament de Riberola

Capçalera del document complet de la Política de Seguretat:

Codi:	SGSI-POLITICA-SEGURETAT
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	18/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Baix

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document – Nova Política
-	-	-	-

A1.1.1 APROVACIÓ I ENTRADA EN VIGOR

Text aprovat per la Junta de Govern Local de l'Ajuntament de Riberola, el dia X de X del X.

La present Política de Seguretat és efectiva des de l'esmentada data fins que no sigui substituïda per una nova política o una nova versió del present document.

L'entrada en vigor de la present Política de Seguretat de la Informació deroga qualsevol altra Política de Seguretat de la Informació que existís en anterioritat.

A1.1.2 OBJECTIUS I MISSIÓ DE L'AJUNTAMENT

L'Ajuntament de Riberola és una administració pública d'àmbit local, els objectius de la qual són, dins el marc de les seves competències, promoure activitats i prestar serveis públics que contribueixen a satisfer les necessitats i aspiracions dels ciutadans de Riberola.

L'organització exerceix les seves competències en els termes previstos en la legislació estatal de l'Estat i de la Comunitat Autònoma de Catalunya.

Per exercir les competències municipals, l'Ajuntament de Riberola fa ús de sistemes d'informació que han de ser protegits d'una forma efectiva i eficient.

A1.1.3 OBJECTIUS I MISSIÓ DE LA POLÍTICA DE SEGURETAT

Un dels principals objectius per la implantació d'un Sistema de Gestió de Seguretat de la Informació és el d'assentar unes bases sobre les quals els treballadors públics i els ciutadans

puguin disposar d'accés als diferents serveis oferts per l'Ajuntament en un entorn de gestió segur, preservant els seus drets.

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

La gestió de la seguretat de la informació ha de garantir el funcionament adequat de les activitats de control, monitorització i manteniment de les infraestructures i instal·lacions, necessàries per proporcionar un servei adequat i de qualitat, així com de la informació derivada de les activitats esmentades.

Per tal de realitzar aquesta gestió, s'estableixen els següents objectius en matèria de seguretat de la informació:

1. Contribuir des de la gestió de la seguretat de la informació a complir amb la missió i objectius establerts per l'Ajuntament de Riberola.
2. Disposar de les mesures de control necessàries pel compliment dels requisits legals que siguin d'aplicació com a conseqüència de l'activitat desenvolupada, especialment en els processos relacionats amb la protecció de dades de caràcter personal i la prestació de serveis a través de mitjans electrònics.
3. Assegurar l'accés, integritat, confidencialitat, disponibilitat, autenticitat, traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb celeritat davant d'incidents.
4. Protegir la informació de l'Ajuntament de Riberola i la tecnologia utilitzada pel ser processament, contra amenaces, internes o externes, deliberades o accidentals, amb la finalitat d'assegurar el compliment de la confidencialitat, integritat, disponibilitat, i legalitat de la informació.

Aquesta Política de Seguretat assegura un **compromís manifest de la Junta de Govern Local de l'Ajuntament de Riberola** per a la difusió, consolidació i compliment de la present Política.

A1.1.4 ABAST

Aquesta Política s'aplica a tots els Departaments Municipals de l'Ajuntament de Riberola, Organismes Autònoms, Societats Municipals amb majoria de capital social municipal i altres entitats que la Junta de Govern Local decideixi, als seus recursos i als processos afectats pel Real Decret 3/2010, ja siguin interns o externs vinculats a l'entitat mitjançant contractes o

acords amb tercers.

A1.1.5 MARC NORMATIU

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

- Llei 7/1985, del 2 d'abril, Reguladora de les Bases del Règim Local.
- Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal i les seves normes de desenvolupament.
- Llei 30/1992, del 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú.
- Llei 34/2002, de l'11 de juliol, de serveis de la societat de la informació i del comerç electrònic.
- Llei 32/2003, del 3 de novembre, General de Telecomunicacions.
- Llei 59/2003, del 19 de novembre, de signatura electrònica.
- Llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 25/2007, del 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.
- Llei 37/2007, del 16 de novembre, respecte la reutilització de la informació del sector públic.
- Llei 56/2007, del 28 de desembre, de Mesures per l'Impuls de la Societat de la Informació.
- Real Decret 1720/2007, del 21 de desembre, pel qual s'aprovà el Reglament de desenvolupament de la Llei Orgànica 15/1999, del 13 de desembre, de protecció de dades de caràcter personal.

A1.1.6 REVISIÓ DE LA POLÍTICA DE SEGURETAT

La Política serà revisada com a mínim un cop l'any, i sempre que hi hagi canvis significatius en l'organització municipal, amb la finalitat d'assegurar que la present Política s'adequa a l'estratègia i necessitats de l'organització.

La Política serà proposada pel **Comitè de Seguretat de Tecnologies de la Informació i Comunicació** (Comitè STIC) i aprovada per la **Junta de Govern Local**.

A1.1.7 ORGANITZACIÓ DE LA SEGURETAT

L'organització de la seguretat queda establerta mitjançant la identificació i definició de les

diferents activitats i responsabilitats en matèria de gestió de seguretat dels sistemes i la implantació d'una infraestructura que els suporti.

A1.1.7.1 Comitès: Funcions i responsabilitats

A continuació es detallen els diferents comitès i les seves funcions i responsabilitats:

a) Junta de Govern Local

En matèria de seguretat en la informació, la Junta de Govern Local de l'Ajuntament de Riberola té les següents funcions:

- Aprovar la Política de Seguretat de la Informació de l'Ajuntament de Riberola.
- Constituir i realitzar el nomenament dels integrants del Comitè de Seguretat en Tecnologies de la Informació i la Comunicació.
- Aprovar les normatives proposades pel Comitè de Seguretat en Tecnologies de la Informació i la Comunicació.
- Adoptar les mesures pertinents, en matèria de seguretat de la informació, a proposta del Comitè de Seguretat en Tecnologies de la Informació i la Comunicació.
- Promoció de la Seguretat com a punt de l'agenda del Govern Municipal.
- Seguiment del quadre de comandament de la seguretat de la informació, per tal de tenir constància tant de la seva evolució i millora, com de les seves possibles deficiències (en general).

b) Comitè de Seguretat en Tecnologies de la Informació i la Comunicació

Un cop aprovada la Política de Seguretat de la Informació es constituirà el Comitè de Seguretat en Tecnologies de la Informació i la Comunicació (Comitè STIC) designat per la Junta de Govern Local.

El Comitè STIC té les següents funcions:

- Elaborar i proposar la política de seguretat de l'organització municipal, per la seva posterior aprovació per part de la Junta de Govern Local.
- Elaborar i proposar les normes de tipus organitzatiu a nivell de tota l'organització municipal.
- Realitzar l'anàlisi i gestió de riscos, aplicat als sistemes de tractament de la informació.
- Elaborar i proposar el desenvolupament normatiu que permeti, en l'àmbit de

l'organització municipal, el compliment dels Esquemes Nacionals de Seguretat i de Interoperabilitat.

- Velar per a que la seguretat de la informació formi part del procés de planificació de l'organització municipal.
- Constitució i revisió dels nomenaments dels integrants del Comitè de Seguretat en Tecnologies de la Informació i la Comunicació.
- Velar pel compliment de la normativa d'aplicació legal referent a la seguretat de la informació i a la protecció de dades de caràcter personal.
- Coordinar les actuacions de seguretat i donar resposta a les inquietuds de seguretat transmeses pels responsables dels diferents departaments de l'Ajuntament.
- Promoure la difusió i recolzar la seguretat de la informació dins de l'estructura orgànica de l'Ajuntament de Riberola.
- Portar a terme accions de conscienciació, formació i motivació del personal municipal afectat per aquesta Política, respecte la importància de les bases establertes en el marc de la gestió de la seguretat de la informació i sobre la seva implicació en el compliment de les expectatives dels departaments municipals, dels usuaris i dels ciutadans en la protecció de la informació.
- Elaborar i avaluar la Política de Seguretat de la Informació de l'Ajuntament de Riberola i les seves Normes Organitzatives.
- Proposar nous criteris de seguretat: redacció, revisió i avaluació de les normes i pautes de seguretat així com també dels processos de notificació d'incidents de seguretat.
- Avaluar i informar sobre riscos de seguretat en els actius TIC.
- Velar per l'alineació de les activitats de seguretat amb els objectius de l'organització municipal, portant a terme processos de millora continua en els processos de seguretat de la informació.
- Velar per a que la seguretat de la informació formi part del procés de planificació de l'organització municipal.

Prenent com a base aquesta Política, es redactarà un document de seguretat, dins del marc organitzatiu, on s'especifiqui la gestió interna del Comitè de Seguretat, identificant tots els seus membres i enumerant les diferents responsabilitats i

atribucions de cadascun dels seus integrants, així com els mecanismes de coordinació.

A1.1.7.2 Rols: Funcions i responsabilitats

A continuació es detallen els rols que intervenen en el Comitè de Seguretat de les Tecnologies de la Informació i la Comunicació:

- **Coordinador del comitè de Seguretat TIC:** Rol assignat al Regidor de Tecnologies de la Informació i la Comunicació. Necessari per coordinar la Junta de Govern Local i el Comitè de Seguretat, del qual també en formarà part.
- **Responsable de Seguretat de la Informació:** Complirà funcions relatives a la seguretat dels sistemes de la informació i la comunicació de l'Ajuntament de Riberola. Equivalent al 'Responsable de Seguretat' esmentat en l'Esquema Nacional de Seguretat (Real Decret 3/2010). Aquest rol recaurà en el Cap del Departament de Tecnologies de la Informació i la Comunicació. Pertany al Comitè de Seguretat TIC. Entre les seves principals funcions destaquen:
  - Elaboració i proposta de nous objectius o propostes de millora del SGSI.
  - Implantació de directrius i procediments requerits pel Comitè de Seguretat.
  - Coordinació dels diferents departaments en matèria de Seguretat en les TIC.
  - Gestió de riscos de nous projectes.
  - Revisió periòdica de l'estat de la seguretat tant en aspectes tècnics com en aspectes organitzatius.
  - Elaboració i gestió de plans de continuïtat dels serveis de l'organització.
  - Mitjançant consultes amb el Secretari de l'Ajuntament, vetllar pel compliment de la legislació vigent en matèria de seguretat de les tecnologies de la informació i la comunicació.
  - Implantació de controls de seguretat.
- **Responsable de Xarxes i Sistemes:** Pertany al Comitè de Seguretat TIC. Aquest rol és equivalent al “Responsable de sistema” que s'esmenta en l'Esquema Nacional de Seguretat (Real Decret 3/2010). Realitzarà les següents accions:
  - Serà l'encarregat de cobrir els requeriments establerts per l'especificació, el disseny, desenvolupament, operació, administració i comunicació de sistemes i recursos de tecnologia.
  - Implementació de les mesures de seguretat en totes les fases i processos dels

sistemes seguint una metodologia de cicle de vida apropiada.

- Realitzarà el seguiment de l'estat de la seguretat dels sistemes d'informació per tal de reduir el risc, sempre i quan estigui al seu abast.
- Col·laborarà en el seguiment dels diferents controls de seguretat dels sistemes del qual n'és responsable.
- Vetllarà pel compliment de les polítiques, normes i revisions vinculades a la seguretat de la informació.
- Aplicació de possibles accions correctores o millores per tal de gestionar els riscos dels diferents actius o millorar algun aspecte de la seguretat de l'organització.

A1.1.7.3 Procediments de designació

La regidoria de Tecnologies de la Informació i Comunicació, a instància de la Junta de Govern Local, crea el Comitè de Seguretat de Tecnologies de la Informació i Comunicació. La proposta de composició del Comitè la realitzarà el Regidor de Tecnologies de la Informació i Comunicació.

Un cop aprovada la Política de Seguretat de la Informació, la Junta de Govern Local crearà el Comitè de Seguretat en Tecnologies de la Informació i Comunicació i designarà els seus components per l'exercici de les competències definides en la present política.

La Junta de Govern Local podrà revisar els nomenaments del Comitè de Seguretat en Tecnologies de la Informació i Comunicació quan ho estimi oportú.

Es nomenarà a personal qualificat, pertanyent a la plantilla actual dels Departaments Municipals, per exercir cadascun dels rols identificats dins del Comitè de Seguretat en Tecnologies de la Informació i Comunicació.

En cas de conflictes o possibles diferents interpretacions de la Política de Seguretat, es recorrerà a la Junta de Govern Local per la seva resolució.

A1.1.8 ANÀLISI I GESTIÓ DELS RISCOS

Tots els sistemes als que aplica la present Política hauran de ser sotmesos a un anàlisi i gestió de riscos, avaluant els actius, amenaces i vulnerabilitats a les que estan exposats i es proposaran contramesures adequades per a reduir-ne el risc.

Tot i que es precisa d'un control continu dels canvis realitzats en els sistemes, aquest anàlisi es repetirà:

- Anualment (mitjançant revisió i aprovació formal).

- Quan succeeixi un accident greu de seguretat.

Per poder prendre mesures estàndard durant l'anàlisi de riscos, el Comitè de Seguretat en Tecnologies de la Informació i la Comunicació utilitzarà una valoració de referència, mitjançant rangs, pels diferents tipus d'informació tractats i els diferents serveis oferts.

Per l'anàlisi i gestió de riscos s'emprarà la metodologia MAGERIT versió 3 (Metodologia per l'Anàlisi i Gestió de Riscos en Sistemes d'Informació), elaborada pel Consell Superior d'Administració Electrònica i enfocada a les Administracions Públiques.

El Comitè de Seguretat en Tecnologies de la Informació i la Comunicació traslladarà a la Junta de Govern Local les necessitats d'inversió en matèria de seguretat de la informació detectades durant la realització dels diferents anàlisis.

A1.1.9 DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

La Política de Seguretat de l'Ajuntament de Riberola es desenvoluparà mitjançant normatives de seguretat que tractin aspectes més específics. S'utilitzaran els següents instruments:

- **Normes de seguretat:** Uniformitzen l'ús d'aspectes concrets del sistema. Indiquen l'ús correcte dels sistemes de l'organització i les diferents responsabilitats dels usuaris. Són de caràcter obligatori. També es poden anomenar Polítiques de Seguretat.
- **Procediments de seguretat:** Tenen caràcter informatiu i el seu objectiu és proporcionar als usuaris mètodes per aplicar correctament les mesures de seguretat.
- **Procediments operatius de seguretat (POS):** Serveixen per a realitzar tasques concretes, indicades pas a pas. Útils per a tasques repetitives i periòdiques.
- **Instruccions tècniques (IT):** Desenvolupen els procediments operatius de seguretat, essent molt més detallades i específiques. Poden contenir referències a uns proveïdors en concret, comandes tècniques per a realitzacions de tasques concretes.

A1.1.9.1 Estructura general

El desenvolupament d'aquesta política inclourà, basant-se en l'anàlisi de riscos, aspectes específics de la Seguretat de la Informació tals com les mesures de seguretat indicades en la norma **ISO/IEC 27001**, les quals es poden alinear amb les indicades en l'Annex II de l'**Esquema Nacional de Seguretat** (presentades a continuació):

a) **Marc organitzatiu:** orientat a administrar la seguretat de la informació dins l'organització municipal i facilitar-ne a gerència el control i implementació. Partint de la present Política de Seguretat es desenvoluparà la resta del marc organitzatiu.

b) **Marc operacional:** conté les mesures a prendre per protegir l'operació del sistema

com a conjunt integral de components per un fi concret.

- **Planificació:** mitjançant anàlisi de riscos, controlant l'arquitectura de seguretat i l'adquisició de nous elements, entre altres aspectes.
- **Control d'accés:** control d'accés lògic a la informació.
- **Explotació:** mesures per a la gestió de la seguretat en explotació, partint de l'inventari d'actius i controlant la gestió d'incidències, canvis, gestió de configuracions i registres d'activitat entre d'altres.
- **Serveis externs:** mesures de seguretat orientades a garantir que empreses i terceres persones que realitzen serveis de qualsevol tipus per l'Ajuntament de Riberola o que d'alguna manera es prestin sota el control i/o direcció de l'Ajuntament compleixin les polítiques i normes de seguretat de la informació establertes per l'Ajuntament.
- **Continuïtat del servei:** accions a executar en cas de patir alguna interrupció de servei en algun dels sistemes.
- **Monitorització del sistema:** orientat a garantir la disponibilitat de les activitats diàries i protegir els processos crítics dels efectes que poden produir incidents o desastres.

c) **Mesures de protecció:** per a protegir actius concrets, segons la seva naturalesa.

- **Protecció de les instal·lacions i infraestructures:** mesures destinades a no permetre l'accés no autoritzat, danys i interferències a les instal·lacions i infraestructures de l'Ajuntament de Riberola.
- **Gestió del personal:** mesures orientades a reduir el risc d'errors humans o ús inadequat dels sistemes.
- **Protecció dels equips:** mesures per a protegir els equips.
- **Protecció de les comunicacions:** mesures per a garantir la seguretat i el bon funcionament dels sistemes de comunicació.
- **Protecció dels suports d'informació:** per garantir la seguretat i confidencialitat de la informació que contenen.
- **Protecció de les aplicacions informàtiques:** orientat a garantir la incorporació de mesures de seguretat en els sistemes d'informació des de el seu desenvolupament i/o implementació i durant el seu manteniment.
- **Protecció de la Informació:** compliment de la Llei Orgànica de protecció de

dades de caràcter personal 11/2007 i gestió de la informació en funció de la seva classificació.

- **Protecció dels serveis:** definició de les mesures necessàries per a mantenir la seguretat dels serveis oferts.

La normativa de seguretat estarà a disposició de tots els membres de l'organització municipal que necessitin conèixer-la. En particular, aquells treballadors que utilitzin, operin o administrin els sistemes d'informació i comunicació.

A1.1.9.2 Sancions previstes per incompliment

L'incompliment de la Política de Seguretat de la Informació tindrà com a resultat l'aplicació de diverses sancions, segons la magnitud i les característiques dels preceptes incomplerts.

El procediment i les sancions a aplicar seran les establertes en la legislació sobre règim disciplinari de les Administracions Públiques.

A1.1.10 SEGURETAT DE LA INFORMACIÓ

Tot i que la seguretat de la informació no és el mateix que la seguretat de les Tecnologies de la Informació i la Comunicació, ambdós estan críticament vinculades. La classificació de la informació de caràcter personal en nivell alt, mitjà o baix no és una qüestió tècnica ni tecnològica, però un cop determinat el nivell de seguretat d'unes dades, aquesta informació requereix un determinat tractament per la seva correcta manipulació.

La classificació de la informació de caràcter personal està estipulada en el Real Decret 1720/2007, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999 de protecció de dades de caràcter personal (LOPD).

Per a la resta d'informació, fora del marc de la LOPD, se'n realitzarà la classificació atenent a la importància o sensibilitat del sistema.

En funció de les diferents exigències de seguretat de la informació, els diferents departaments de l'Ajuntament de Riberola classificaran la informació en: **Confidencial**, **difusió limitada**, **sense classificar** i **pública**. Tota la documentació, ja sigui digital o impresa, ha de portar indicada la seva classificació sempre que no sigui **pública**.

Aquesta classificació de la informació ha de tenir en compte les conseqüències que es derivarien del seu coneixement per persones que no haurien de tenir-hi accés.

A1.1.11 DADES DE CARÀCTER PERSONAL

L'Ajuntament de Riberola està format per diferents entitats i societats municipals. Per

tant, no existeix un únic document de seguretat, sinó que n'existeix un per cadascuna de les entitats.

L'Ajuntament apareix com a prestador de serveis per aquestes entitats, ja que utilitzen la infraestructura, sistemes i personal per la gestió de la seva informació i les seves comunicacions.

El Departament de Tecnologies de la Informació i Comunicació és l'encarregat de gestionar aquests documents de seguretat.

El Comitè de Seguretat podrà dictar noves formes d'actuació en matèria de protecció de dades de caràcter personal.

A1.1.12 OBLIGACIONS DEL PERSONAL

Tots els membres de l'organització municipal i les empreses i terceres persones que realitzen serveis de qualsevol tipus contractats per l'Ajuntament de Riberola, o que d'alguna manera estiguin sota la direcció de l'Ajuntament tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, que serà proporcionada per part dels diferents Departaments Municipals, els quals disposaran dels mitjans necessaris per a fer arribar la informació als afectats.

S'establirà un programa de conscienciació contínua dirigit a tots els membres de l'Ajuntament, en especial als de nova incorporació.

El personal haurà de fer ús dels procediments de notificació habilitats en cas de detectar alguna incidència.

Les persones amb responsabilitats en l'ús, operació i administració de sistemes d'informació rebran formació per gestionar els sistemes de manera segura.

A1.1.13 TERCERES PARTS

Quan l'Ajuntament de Riberola utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partíceps d'aquesta Política de Seguretat i de la Normativa de Seguretat que afecti als serveis tractats. Aquest tercer haurà d'acceptar les obligacions establertes en la normativa. S'establiran procediments específics d'informació i notificació d'incidències.

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

A1.2 PROCEDIMENT D'AUDITORIES INTERNES

Capçalera:

Codi:	SGSI-PROCS-AUDIT-INTERNES
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	18/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document
-	-	-	-

A1.2.1 OBJECTIUS I ABAST

Aquest procediment inclou la planificació, execució i elaboració d'informes i seguiments de l'auditoria interna del Sistema Gestor de Seguretat de la Informació de l'Ajuntament de Riberola.

La realització periòdica d'aquest tipus d'auditories, en aquest cas anualment, serveixen per assegurar que l'organització segueix operant en el marc de les polítiques, procediments i requeriments externs establerts per tal de garantir els objectius de l'Ajuntament en matèria de Seguretat de la Informació. Addicionalment, també faciliten l'aplicació de millores al Sistema Gestor de Seguretat de la Informació.

A1.2.2 ROLS I RESPONSABILITATS

Existeixen tres rols a tenir en compte en aquest procediment:

a) **Auditor en cap**

- Prepara el pla d'auditoria
- Lidera les activitats de l'auditoria interna del SGSI.
- Coordina el pla d'auditoria amb els caps dels departaments afectats.

- Planifica l'auditoria i coordina l'equip d'auditors.
- Consolida totes les no conformitats i observacions i prepara l'informe.
- Informa a l'auditat immediatament de no conformitats crítiques del sistema.
- Està present en les reunions d'inici i final del procés d'auditoria interna.

b) Membre de l'equip d'auditors

- Dóna suport al cap d'auditors per la realització de les diferents activitats.
- Realitza l'auditoria utilitzant una llista de verificació d'auditoria consolidada.
- Informa de les no conformitats i recomana possibles actuacions.

c) Auditat (organització)

- Rep, considera i opina respecte l'informe d'auditoria.
- Determina, proporciona recursos, dirigeix i completa accions correctives.

A1.2.3 PROCEDIMENT

A1.2.3.1 General

- Cal crear un programa d'auditories que contindrà la programació de totes les possibles auditories a realitzar durant l'any.
- Només podrà ser duta a terme per personal capacitat i totalment independent a l'àrea que cal auditar.
- L'auditor en cap supervisarà les actuacions de l'equip d'auditoria.

A1.2.3.2 Planificació i preparació de l'auditoria

- Cal realitzar una auditoria interna com a mínim un cop l'any.
- Cal avisar amb un mes d'antelació als departaments per tal d'estar preparats per rebre l'auditoria.
- Prèviament a la realització es revisaran els objectius amb el Comitè de Seguretat de l'Ajuntament de Riberola.
- L'auditor en cap adaptarà la modificació dels objectius en cas de ser necessari.
- El pla d'auditoria, un cop realitzat per part de l'auditor en cap, serà comunicat al Comitè de Seguretat i a l'equip d'auditors. El pla ha d'incloure els següents punts:
    - Objectiu i abast de l'auditoria

- Departaments i responsables dels departaments
- Membres de l'equip d'auditoria
- Distribució de dates, hores i llocs per realitzar activitats de l'auditoria

A1.2.3.3 Reunió prèvia

- Es realitzarà com a mínim una reunió prèvia entre el cap d'auditors i el responsable de seguretat de l'organització amb els següents objectius:
  - Assegurar la disponibilitat dels recursos tècnics i humans necessaris que poden ser requerits per l'equip d'auditoria.
  - Verificació dels objectius i abast de l'auditoria.

A1.2.3.4 Reunió d'inici

- Es realitzarà uns dies abans de l'inici de l'auditoria. Intervindran el cap de seguretat i el cap d'auditors per tal de tractar:
  - Confirmació del pla d'auditoria.
  - Resolució dels possibles dubtes que puguin aparèixer abans d'iniciar l'auditoria.

A1.2.3.5 Execució d'auditoria

- L'equip d'auditors realitzarà l'auditoria utilitzant les següents llistes de verificació:
  - **Llista de verificació d'auditoria interna / Formulari d'observacions:** conté elements específics de l'organització per ser auditats. Els auditors generant les qüestions pertinents utilitzant aquest formulari.
  - **Llista de verificació de requeriments sistemàtics:** conté elements relacionats amb amb els requeriments de la ISO/IEC 27001.
  - **Llista de verificació de controls:** conté els elements que pertanyen als diferents controls descrits en la ISO/IEC 27002.
- Les conclusions dels auditors vindran de les diferents entrevistes realitzades al personal de l'organització, així com també de l'examinació de documentació existent, l'observació de les activitats i de les condicions de les àrees que estan afectades pel pla d'auditoria. Aquestes conclusions es veuran reflectides en les diferents llistes de verificació comentades en l'apartat anterior.
- L'evidència de l'existència d'altres no conformitats cal que siguin anotades, tot i que

no pertanyin o estiguin vinculades a cap llista de verificació.

A1.2.3.6 Informe d'auditoria

- L'equip d'auditoria es reunirà un cop recollides totes les evidències i observacions per tal de:
  - Revisar, analitzar i consolidar les dades recollides.
  - Classificació de les diferents no conformitats o observacions.
  - Preparació de l'informe d'auditoria i de les recomanacions segons els resultats.
- Totes les observacions i no conformitats que s'indiquin a l'informe cal que vagin acompanyades per evidències objectives.
- L'auditor en cap consolidarà totes les no conformitats i observacions.
- La classificació de les no conformitats o observacions serà la següent:
  - **No conformitat greu:** deficiència greu en algun element que provoca un efecte directe en la preservació de la confidencialitat, integritat o disponibilitat d'algun element o sistema. Requereix d'una acció correctiva.
  - **No conformitat lleu:** deficiència menor que fa que un element només compleixi parcialment amb el que precisa. Té un efecte indirecte en la seguretat de la informació. Requereix d'una acció correctiva.
  - **Potencial de millora:** millora que pot ser implementada o no per l'auditat, però que milloraria l'element indicat.
  - **Observacions positives:** observacions d'elements que es troben en una situació molt més bona que la requerida.
- L'auditor en cap prepararà un informe d'auditoria que ha de contenir, com a mínim, els següents punts:
  - Número de referència d'auditoria.
  - Data de l'auditoria.
  - Departaments, seccions i processos auditats.
  - No conformitats i observacions.
  - Referència al SGSI i a l'estàndard ISO/IEC 27001.
  - Accions preventives i correctives a realitzar amb data de previsió.

- Seguiment per les no conformitats reportades.
- Verificació dels diferents seguiments.

- Els auditors han de seguir les següents premisses per a la realització dels informes:
  - L'informe ha de ser concís però realitzat i presentat de manera constructiva.
  - Els resultats han d'estar dins l'abast de l'auditoria i han de mostrar la relació amb l'estàndard utilitzat.
  - Ha de ser objectiu i no es pot desviar segons subjectivitats de l'auditor.

A1.2.3.7 Reunió final

- L'auditor en cap presidirà una última reunió entre el Comitè de Seguretat de les Tecnologies de la Informació i la Comunicació de l'Ajuntament de Riberola.
- L'equip d'auditors informarà dels resultats de l'auditoria interna, les observacions i les recomanacions, resumint els punts correctes per passar posteriorment a comentar les diferents no conformitats trobades.
- Totes les parts hauran preservaran la confidencialitat de les dades i resultats obtinguts.

A1.2.4 SEGUIMENT DE L'AUDITORIA I FINALITZACIÓ

- Així com l'equip d'auditoria és responsable d'identificar les diferents no conformitats, l'organització serà la responsable de resoldre les no conformitats reportades.
- Les accions correctives seran planificades o previstes en comú acord entre el Comitè STIC i l'equip d'auditors.
- L'auditoria no es considerarà finalitzada fins que totes les mesures correctives o preventives no hagin estat implementades. L'auditor en cap en realitzarà la supervisió.

A1.2.5 QUALIFICACIÓ DELS AUDITORS

- Cal que els auditors estiguin capacitats personal i professionalment per tal de realitzar les diferents tasques d'auditoria. Per tant, hauran de tenir coneixements de les següents àrees:
  - Principis d'auditoria, coneixements i tècniques.
  - Sistemes de Gestió de Seguretat de la Informació i documents de referència.
  - Coneixements bàsics de l'Administració Pública i les seves funcions.

- Legislació i regulació vigent en relació a la seguretat de la informació.

A1.2.6 REGISTRES

- A més de les evidències de l'auditoria interna, com per exemple còpies de documents, anotacions, entrevistes, registres de sistemes, etc., l'auditoria interna d'un SGSI genera els següents registres:
  - Programa d'auditoria.
  - Planificació de l'auditoria.
  - Llistes de verificació.
  - Informe d'auditoria interna.
  - Informe de no conformitats, accions correctives i preventives.
- Tota la informació rebrà un tracte confidencial, degut a la seva naturalesa.
- Tota la informació serà degudament emmagatzemada i indexada.
- Se'n farà referència al SGSI de l'organització.

A1.3 FITXA D'INDICADOR

Capçalera:

Codi:	SGSI-INDIC-DETALL-**[NOM]**
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	18/03/2013
Aprovat per:	Comitè de Seguretat
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document
-	-	-	-

Contingut:

Nom de l'indicador:	Nom de l'indicador
Descripció:	Descripció de l'indicador. Cal indicar-ne l'objectiu de manera clara.
Control(s) relacionat(s):	- Control 1 - Control 2 - ...
Fórmula de mesurament:	Explicació amb la fórmula de mesurament. Paràmetres d'entrada objectius i concrets. No amigüitats.
Unitats de mesura:	Indicar les unitats de mesura per l'indicador actual.
Freqüència de mesura:	Setmanal, quinzenal, mensual, trimestral, ...
Valor objectiu / llindar:	Valor objectiu / valor llindar (si és possible)
Responsable de la mesura:	Departament i responsable dins del departament encarregat de realitzar les mesures periòdicament.

Nota: Es podrà disposar d'algun document índex per tal de relacionar de manera directa i ràpida els indicadors que pertanyen a cada control. Tot i així es requerirà que la descripció dels indicadors segueixi constant apart, juntament amb la seva descripció i definició.

A1.4 INDICADORS PER OBJECTIU DE CONTROL

Els indicadors implementats o a implementar per revisar els diferents controls i/o objectius de control dels dominis de la ISO.

Capçalera:

Codi:	SGSI-LLISTA-INDICADORS
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	29/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document

-	-	-	-

Llista dels diferents indicadors (per cadascun hauria d'existir un document com l'indicat en el punt anterior), on s'amplia la seva descripció i característiques, així com la tolerància definida per l'indicador (en negreta):

5. POLÍTICA DE SEGURETAT		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
5.1 Política de seguretat de la informació		
5.1.1 Document de política de seguretat *	Pendent de revisió i aprovació per JGL. Proposta adjunta en projecte TFM.	% de polítiques redactades, revisades i aprovades del total de l'estàndard. **Tolerable a partir del 60%.**
5.1.2 Revisió de la política de seguretat	Establiment periodicitat de revisió/aprovació.	Número de trobades de revisió dividit pel total previstes. **Tolerable a partir 85%.**
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
6.1 Organització interna		
6.1.1 Comitè de seguretat	Pendent de formació. Documentat en proposta en projecte TFM.	# de sessions realitzades dividit per semestres. **Tolerable a partir si # > 2.**
6.1.2 Coordinació	En la definició de rols i funcions proposada en aquest TFM hi ha una proposta. Cal revisió i aprovació.	Número de reunions de coordinació dividit pel total previstes (o freqüència anual). **Tolerable si > 85%.**
6.1.3 Assignació de responsabilitats *	Definició formal en document actual. Cal revisió i aprovació.	Entrevistes a personal respecte responsabilitats. Mitja dels resultats obtinguts. **Tolerable si resultat per sobre del 70% encerts.**
6.1.4 Autorització de recursos	Pendent de realitzar. Cal que existeixi el document pertinent.	Entrevistes a personal respecte procediments. Mitja ponderada dels resultats . **Tolerable si**

		resultat per sobre del 70% encerts.
6.1.5 Acords de confidencialitat	Al ser administració pública tots els serveis van regulats per convenis o contractes.	Revisió de 5 contractes de l'any en curs aleatoris i comprovació de % d'existència d'acords. **Resultat ha de ser 100% encerts. Requisit legal.**
6.1.6 Contacte amb autoritats	Implementat. Procediment Policia local – Mossos d'esquadra. Contactes INTECO i CESICAT.	Entrevistes personal respecte procediments de contacte amb autoritats. Mitja ponderada dels resultats. **Tolerable per sobre del 70% encerts.**
6.1.7 Contacte amb altres grups d'interès	L'organització està en llistes de INTECO-CERT i CESICAT, entre altres.	Entrevista respecte procediments de captació d'informació d'aquests grups. **Tolerable per sobre del 70% encerts.**
6.1.8 Revisió independent	No es preveu pròximament. Cal contractar empresa externa per auditoria / revisió del SGSI.	# d'auditories realitzades anuals / previstes per l'estàndard. **Tolerable només si es realitzen totes.**
6.2 Tercers		
6.2.1 Identificació de recursos	Subconjunt de l'inventari d'actius, serveis gestionats per empreses externes.	% de tercers amb polítiques de seguretat establertes o compliment d'estàndard ISO27001. **Tolerable per sobre del 50%.**
6.2.2 Seguretat en la relació amb clients	Aplica la LOPD per la relació amb els clients, en el nostre cas la ciutadania.	
6.2.3 Seguretat en acords amb terceres parts	En cas de serveis TIC, sempre es preveuen els punts de seguretat en els diferents contractes. Existeix, però no està documentat actualment.	
7. GESTIÓ D'ACTIUS		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
7.1 Responsabilitats sobre els actius		

7.1.1 Inventari d'actius	Mitjançant Magerit. Identificació d'actius present en aquest document.	% d'elements inventariats en cada classificació (identificat, inventariat, etc.). **Tolerable per sobre del 90%.**
7.1.2 Propietat dels actius	En la documentació dels actius ha de constar el propietari(s).	Entrevistes a propietaris per captar si s'assumeixen les responsabilitats pertinents. **Respostes de qüestionari amb encerts en més del 70%.**
7.1.3 Ús acceptable dels actius	Generació de documents de polítiques d'ús (i aplicació). Polítiques en Active Directory, Tallafocs i Proxy.	Revisió de cadascun dels punts de les polítiques i establiment d'un nivell de maduresa CMMI. **Tolerable si valoració mitja de punts > L4.**
7.2 Classificació de la Informació		
7.2.1 Guies de classificació	Acció realitzada per adaptació a la LOPD. Consultar Document de Seguretat.	% d'informació classificada en alguna categoria respecte del total. **Tolerable per sobre del 60%.**
7.2.2 Marcatge i tractament de la informació	La informació es tracta actualment segons classificació. Pendent etiquetar.	
8. SEGURETAT RELATIVA AL PERSONAL		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
8.1 Abans de la contractació		
8.1.1 Rols i responsabilitats	Comunicació de polítiques de seguretat en paper i versió electrònica a candidats i empreses.	Entrevista a recursos humans respecte procediments de contractació de personal. Mitja ponderada dels resultats. **Tolerable si % > 70%.**
8.1.2 Selecció i política de personal	Al ser administració pública es realitzen les verificacions pertinents, siguin processos d'empreses o particulars.	
8.1.3 Termes i condicions de la relació laboral	Introducció en el contracte de clàusula d'acceptació de polítiques de seguretat.	

8.2 Durant la relació laboral		
8.2.1 Supervisió d'obligacions	Signatura de clàusula en contractes i convenis.	% d'empleats que han rebut formació durant l'any. **Tolerable per sobre del 65%.**
8.2.2 Conscienciació, formació i capacitació en seguretat *	Es precisa de planificació periòdica de formació. Dotació de pressupost anual.	
8.2.3 Procediment disciplinari	Està formalitzat en les bases de l'administració local.	Entrevista a personal de secretaria respecte procediments disciplinaris. # de procediments / total d'empleats. **Valoració d'encerts per sobre del 70% (nota absoluta > 7).**
8.3 En finalitzar la contractació o canvi d'ocupació		
8.3.1 Cessació de responsabilitats	Existeix, però no està documentat actualment.	Entrevista (qüestionari) de procediment de cessió en recursos humans i càlcul de mitja. **Tolerable per sobre del 7 (70% encerts).**
8.3.2 Devolució d'actius	Document signat conforme se li proporciona, i que cal tornar-lo un cop finalitzada l'activitat.	# Actius retornats / treballadors que han cessat activitat i que disposaven d'algun actiu. **Tolerable per sobre del 90%.**
8.3.3 Eliminació de drets d'accés	Personal comunica baixes en correu electrònic a Responsable de seguretat.	% ex-empleats que encara apareixen en alguns registres d'accés. **Tolerable per sota del 5%.**
9. SEGURETAT FÍSICA I DE L'ENTORN		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
9.1 Àrees segures		
9.1.1 Perímetre de seguretat física	Es disposa d'accés autenticat amb codi, taulells de recepció i portes amb pany (clau) en les diferents dependències.	Utilització del nivell de maduresa CMMI. **Tolerable per sobre de L4.**
9.1.2 Control d'accés físic	Els tres CPD estan darrera de portes tancades amb clau.	Utilització del nivell de maduresa CMMI.

		Acceptable per sobre de L4.
9.1.3 Seguretat en oficines, despatxos i recursos	Presència de gent constant i dispositius de perímetre punt 9.1.1 per fora horari.	Entrevistes a personal respecte procediments diaris. Observacions i informes. Mitja puntuable. **Acceptable si nota > 7 (encerts > 70%).**
9.1.4 Protecció enfront d'amenaces externes i d'entorn	Existència d'extintors de diferents tipus segons actius propers.	Número de revisions d'extintors i detecció de fums. Utilització del nivell de maduresa CMMI per altres amenaces. **Tolerable si nivell CMMI > L4.**
9.1.5 El treball en àrees segures	No es requeriex.	N/A
9.1.6 Accés públic, zones de càrrega i descàrrega	No es requeriex.	N/A
9.2 Seguretat en equips		
9.2.1 Ubicació i protecció	Protecció de servidors i commutadors dins armaris RACK. Cal procediment per estacions de treball i altres elements menys crítics.	Valoració de situació segons nivell de maduresa CMMI. **Acceptable si nivell CMMI > L4.**
9.2.2 Subministraments	Els CPD disposen de SAIs. Pendent SAI per un mínim d'estacions de treball.	Número de talls de corrent anuals que afectin els serveis. **Acceptable si menor o igual a 2.**
9.2.3 Seguretat del cablejat	Desplegament de cablejat ethernet en paret i fibra òptica en rasa sempre que sigui possible.	Número d'incidències derivades del cablejat (anual). **Tolerable si < 2.**
9.2.4 Manteniment dels equips	Es disposa de contractes de manteniment en serveis centrals. Tasques menors en altres elements.	Número d'incidències anuals en referència als equips. % temps de disponibilitat. % de sistemes amb garantia de fabricant respecte el total. **Mitja dels tres valors > 70%.**

9.2.5 Seguretat fora dels locals	Portàtils, memòries USB i telèfons amb codis d'accés i si és possible, partició xifrada de dades per emmagatzemar informació.	Número d'incidents de seguretat fora locals (anualment). **Acceptable si menor de 10.**
9.2.6 Reutilització o eliminació	Contractació d'empresa externa puntualment per destrucció d'elements presumibles de contenir dades.	Número d'eliminacions realitzades (pes o elements eliminats) durant període. **Tolerable si major de 2 cops (anualment).**
9.2.7 Autorització de sortida	No existeix actualment cap procediment similar. Cal redactar, revisar i aprovar el document.	Revisió d'últims procediments de sortida aleatòriament i entrevistes a personal per avaluar coneixement de procediment. **Tolerable si nota del qüestionari > 7 (encerts > 70%).**
10. GESTIÓ DE COMUNICACIONS I OPERACIONS		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
10.1 Procediments d'operació i responsabilitats		
10.1.1 Documentació de procediments	Pendent d'implementar en la major part de departaments. Cal eina (p.ex. Wiki) i redacció de procediments.	Entrevistes a personal valorades. **Tolerable si nota > 7 (encerts > 70%).**
10.1.2 Gestió de canvis	Eina de gestió documental i GIT o similar pendents d'implementar.	Número de canvis sotmesos en els últims 6 mesos * 100 / modificacions totals. **Tolerable si > 50%.**
10.1.3 Segregació de funcions	Existeixen diferents nivells de treballadors segons les seves funcions en cada departament. Consta en contracte.	Entrevistes a personal valorades. **Tolerable si nota > 7 (encerts > 70%).**
10.1.4 Separació d'entorns desenvolupament i producció	En l'àrea TIC es disposa de maquinari preparat per realitzar d'entorn de proves.	Número de maquinari destinat a desenvolupament / número de maquinari destinat a producció. **Acceptable amb valor per sobre**

		del 50%.
10.2 Gestió de la prestació de serveis per tercers		
10.2.1 Prestació de serveis	Sol·licitar informació periòdicament per part del Responsable de Seguretat.	Número d'entrades en documentació de Seguretat (registre d'activitat). **Tolerable si activitat recent (mínim registre mensual).**
10.2.2 Monitoratge i revisió de serveis	S'utilitza l'eina Nagios per controlar els serveis i elements TIC.	Temps d'activitat de Nagios i número d'incidències reportades. **Acceptable < 3 notificacions setmanals.**
10.2.3 Gestió de canvis en els serveis	Còpia de dades involucrades, execució fora hores d'atenció i en cas de canvi crític, proves en entorn de proves.	Incidències per canvis / Número de canvis realitzats. **Tolerable per sota del 10%.**
10.3 Planificació i acceptació del sistema		
10.3.1 Gestió de la capacitat	Nagios, VMWare i OSSIM IDS permeten la monitorització i control d'aquests recursos i serveis.	Número d'alertes de falta de memòria, CPU i capacitat de disc dels sistemes. **Tolerable per sota de 5 al mes (60/any).**
10.3.2 Acceptació de sistemes	No s'actualitza res dels diferents sistemes fins que el departament TIC no ho aprova.	Revisió aleatòria d'últims canvis acceptats, % canvis documentats del total de canvis realitzats. **Tolerable per sobre del 70%.**
10.4 Protecció conta codi maliciós		
10.4.1 Protecció contra codi maliciós	Es disposa d'antivirus, proxy, firewall i programa anti-malware i IDS. Cal canviar algun sistema antic.	Número d'incidències per virus o codi maliciós. **Tolerable per sota de 20 setmanals**.
10.4.2 Protecció contra codi descarregat en el client	Control tràfic de xarxa (IDS), a més de permisos limitats en estacions de treball per evitar instal·lacions de programari no autoritzat.	# incidències durant període concret respecte instal·lacions indegudes de programari. **Tolerable per sota del 20%.**
10.5 Gestió de suports i recuperació		

10.5.1 Recuperació de la informació	Sistema de còpies de seguretat en cinta, fins a 25 dies d'antiguitat.	Prova de recuperació de 5 elements aleatoris dels últims 25 dies. % de recuperacions efectives. % de còpies correctes. (100 - #% de còpies incorrectes per mesurar efectivitat). **Tolerable si mitja de 3 percentatges > 85%.**
10.6 Gestió de la seguretat de xarxes		
10.6.1 Controls de xarxa	Existència de Tallafocs, Proxy i control de tràfic per IDS (Snort – OSSIM).	Bloquejos de tràfic malèvol del firewall + accessos no permesos en proxy + deteccions anomalies en IDS. **Tolerable si menys de 100 casos anyals seria acceptable.**
10.6.2 Seguretat dels serveis de xarxa	Separació de xarxes i creació de subxarxes. Control de serveis per Nagios.	Número d'incidents de seguretat (IDS) i temps de no disponibilitat del sistema.
10.7 Gestió de suports d'informació		
10.7.1 Gestió de suports extraïbles	Pendent. A incloure en futura wiki de seguretat.	Entrevistes a personal que disposa d'aquest tipus d'actius. **Tolerable si nota > 7 (encerts > 70%).**
10.7.2 Retirada de suports	Eliminació per empresa externa autoritzada i certificada. Igual que en control 9.2.6.	Revisió de registres d'eliminació. Còmput respecte total d'eliminacions. **Tolerable si més de 2 cops cada 6 mesos.**
10.7.3 Procediments d'utilització de la informació	Pendent. A incloure en futura wiki de seguretat.	% de suports extraïbles amb disponibilitat de xifratge respecte el total. **Tolerable per sobre del 80%.**
10.7.4 Seguretat en la documentació dels sistemes	S'emmagatzema en digital, amb restriccions d'accés i en caixa forta de manera física.	Entrevistes a personal encarregat per validar coneixement dels procediments. **Tolerable si nota > 7 (encerts > 70%).**

10.8 Intercanvi d'informació		
10.8.1 Polítiques i procediments d'intercanvi d'informació	Pendent, ja que existeixen però no queden degudament documentats.	Entrevistes a personal i valoracions mitjanes. **Tolerable si nota > 7 (encerts > 70%).**
10.8.2 Acords d'intercanvi	Sempre hi ha una signatura de conveni o contracte on es contemplen aquest tipus de clàusules.	Revisió aleatòria de N contractes. % de contractes on apareix contemplat. **Només acceptable si 100%.**
10.8.3 Suports físics en trànsit	Pendent de realitzar procediment. Actualment no es xifren ni es comprova l'autenticitat.	% de suports xifrats respecte suports enviats. **Acceptable si > 75%.**
10.8.4 Missatgeria electrònica	El servidor disposa d'antivirus i antispam. Les comunicacions requereixen protocol SSL xifrat.	Correus SPAM rebuts. Estadístiques Nagios respecte disponibilitat de correu i port SSL. **SPAM < 5% correus rebuts i disponibilitat correu superior al 98%.**
10.8.5 Sistemes d'informació del negoci	Revisió periòdica de procediments i sistemàtica en canvi de flux de treball.	Entrevistes amb personal i obtenció de mitja valorada. **Tolerable si nota > 7 (encerts > 70%).**
10.9 Serveis de comerç electrònic		
10.9.1 Comerç electrònic	No es requereix.	N/A
10.9.2 Transaccions en línia	No es requereix.	N/A
10.9.3 Informació d'accés públic	Es segueix la LOPD en els diferents processos de l'Ajuntament relacionats amb ciutadans.	Entrevistes amb el personal de l'organització. Qüestions LOPD. Obtenció de mitja. **Tolerable si nota > 7 (encerts > 70%).**
10.10 Monitoratge		
10.10.1 Registre d'activitats	Els realitza, però caldria incrementar nivell de detall.	% de sistemes amb els logs apropiadament configurats, centralitzats de manera segura i
10.10.2 Ús dels sistemes de monitoratge	Els sistemes de procés d'informació estan	

	monitoritzats per Nagios i VMWare. Cal documentar.	monitoritzats correctament. **Tolerable si compleixen més del 85% de sistemes.**
10.10.3 Protecció de les traces i registres	Les dades dels logs i registres han de tenir accés restringit.	
10.10.4 Traces d'administració i operació	Habilitar registres d'auditoria en servidors per qualsevol usuari.	
10.10.5 Registre de fallades	Registres d'error habilitats en el servidor.	
10.10.6 Sincronització de rellotges	Utilització de protocol de xarxa NTP.	Incidències de hores mal configurades anuals. **Acceptable per sota de 15 anuals.**
11. CONTROL D'ACCÉS		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
11.1 Requisits de negoci pel control d'accés		
11.1.1 Política de control d'accés	Implementat mitjançant comptes Active Directory.	Número d'accessos indeguts a informació que no corresponia (per any). **Tolerable si menys de 5 casos anuals.**
11.2 Gestió d'accés dels usuaris		
11.2.1 Registre d'usuaris	Operació realitzable amb Active Directory.	Temps entre petició d'usuari nou i tasca realitzada. **Acceptable si temps mig menor a 4 hores.** Número d'usuaris nous en últim període respecte contractacions. **Acceptable si superior a 85%.**
11.2.2 Gestió de privilegis	Divisió d'usuaris en grups per assignació de permisos. Drets d'operacions respecte grups o usuaris amb AD.	% d'usuaris sense grup assignat. **Tolerable si són menys del 3%.** Temps de procés entre demanda de canvi de permisos i aplicació dels canvis. **Tolerable menys de 4 hores.**
11.2.3 Gestió de contrasenyes d'usuari	Gestió des d'Active Directory.	Número de canvis de contrasenya / número d'usuaris per període de 6 mesos (igual que 11.5.3).

		Acceptable si el valor és major que 1'5.
11.2.4 Revisió dels drets d'accés d'usuari	Tasca a realitzar, cal assignar periodicitat i documentar.	% d'usuaris amb drets concrets respecte usuaris sense cap assignació de permisos. **Tolerable sempre que sigui > 95%.**
11.3 Responsabilitat dels usuaris		
11.3.1 Ús de credencials	Forçat per política AD.	Número d'accessos autenticats / número d'accessos totals a recursos de xarxa. **Tolerable entre 0'90 i 0'95.**
11.3.2 Equips d'usuaris desatesos	Política AD. Bloquejar en 20 minuts d'inactivitat.	Número de polítiques d'AD que contemplen timeouts i bloquejos. **Acceptable si el percentatge de polítiques aplicades actives és superior al 60%.**
11.3.3 Política de taules i pantalles netes	Falta redactar i adoptar política per part de personal.	Entrevista a personal i obtenció de mitja. **Tolerable si nota > 7 (encerts > 70%).**
11.4 Control d'accés a la xarxa		
11.4.1 Política d'ús dels serveis de la xarxa	Autenticació d'usuari en AD directament o per LDAP (Linux).	Estadístiques de tràfic en Tallafocs i en Sistema de detecció d'intrusions. Cercar tràfic i classificar-lo segons control. Control d'autenticacions incorrectes en diferents serveis. **Tolerable per sota del 10% de totes les autenticacions detectades.**
11.4.2 Autenticació d'usuaris per a connexions remotes	Autenticació d'usuari per LDAP (Linux).	
11.4.3 Autenticació de nodes a la xarxa	Configurat en Active Directory.	
11.4.4 Protecció dels ports de diagnòstic i configuració remots	Control de firewall, registres del IDS i controls periòdics exteriors per CESICAT.	
11.4.5 Segregació de les xarxes	Són tot xarxes independents, habilitades per VLAN, tallafocs i routers.	

11.4.6 Control de la connexió a la xarxa	Active directory permet assignar horaris i estacions permeses a usuaris concrets. Pendent millorar les restriccions.	
11.4.7 Control d'encaminament a la xarxa	Routers i tallafocs. IDS per registrar anomalies.	
11.5 Control d'accés al sistema operatiu		
11.5.1 Procediments de connexió segur	Accés autenticat segur amb AD o LDAP amb SSL.	Sistemes amb autenticació xifrada i segura respecte sistemes totals. **Acceptable per sobre del 80%.**
11.5.2 Identificació i autenticació d'usuaris	Implementat en AD, existència d'algun usuari genèric per alguna tasca residual.	Número d'empleats sense usuari ni identificador assignat respecte el total d'empleats. **Acceptable si el nombre és 0.**
11.5.3 Sistema de gestió de contrasenyes	Pendent incrementar polítiques de contrasenyes i habilitació de canvi.	Número de canvis de contrasenya / número d'usuaris per període de 6 mesos (igual que 11.2.3). **Tolerable si el valor és major que 1'5.**
11.5.4 Ús dels serveis del sistema	Sempre es requereix algun tipus d'autenticació.	Número d'autenticacions incorrectes o intents no autoritzats (anualment). **Tolerable per un nombre inferior a 100 (afectat per entrades de comptes incorrectes).**
11.5.5 Desconnexió automàtica de sessió	Actualment algun servei no ho realitza. Cal forçar-ho (aplicació padró i expedients)	Prova de desconnexió/limitació en 5 sistemes aleatoris. % de sistemes que apliquen controls correctament. **Tolerable si compleixen > 80% (pot fallar un sistema dels provats).**
11.5.6 Limitació del temps de connexió	Està habilitat en la major part de servidors. Revisar i configurar la resta.	
11.6 Control d'accés a la informació i a les aplicacions		

11.6.1 Restricció d'accés a la informació	Implementat per AD.	% de plataformes que compleixen amb les línies de seguretat bàsiques de l'estàndard. **Acceptable sempre que sigui > 90%.**
11.6.2 Aïllament de sistemes sensibles	Dos servidors Windows 2003 suporten les dos principals aplicacions de l'organització.	
11.7 Informàtica mòbil i teletreball		
11.7.1 Informàtica mòbil i comunicacions	Pendent realitzar el procediment. Actualment formació puntual en entrega de terminal.	Entrevista a personal per obtenir valoració mitja (CMMI). **Ponderació de nota => nivell CMMI (L1, L2, L3, L4 i L5).** Número d'incidències amb elements mòbils involucrats (anual). **Acceptable per sota de 20 l'any.**
11.7.2 Teletreball	No es requereix.	N/A.
12. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE SISTEMES D'INFORMACIÓ		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
12.1 Requisits de seguretat en sistemes d'informació		
12.1.1 Anàlisi i especificació de requisits	Adjunt en documentació de requeriments.	Model de maduresa CMMI segons revisió de documentació d'anàlisi de requeriments d'últims desenvolupaments (aleatori). **Tolerable per valoracions mitges superior o igual a L4.**
12.2 Control de processos en aplicacions		
12.2.1 Validació de dades d'entrada	Es realitza sempre en la mateixa aplicació, segons tipus de dades a introduir.	Número de procediments o mòduls que passen correctament els test respecte els que no el passen. **Tolerable sempre que el % sigui major a 90%.**
12.2.2 Control de processos interns	No s'està realitzant. Cal realitzar-los segons aplicació.	
12.2.3 Integritat de missatges	Procés de verificació en procés de dades automàtic, segons aplicació.	
12.2.4 Validació de dades de sortida	En aquests processos, es realitza un enviament de	

	correu electrònic amb sortida de la validació.	
12.3 Controls criptogràfics		
12.3.1 Política d'ús de controls criptogràfics	Proveïts per CatCERT, certs usuaris en disposen. Cal amplificar-ne l'ús.	% de sistemes que per les seves dades s'hi ha implementat un control d'accés criptogràfic. **Acceptable si nota > 7 (encerts > 70%).**
12.3.2 Xifratge	Ús de SSL i certificats en certs protocols i serveis.	
12.4 Seguretat dels fitxers de sistema		
12.4.1 Control de programari en producció	Només permès per administradors. Cal crear procediment tot i que es segueixen pautes concretes.	Entrevistes per obtenció de dades i generació de valor mig. **Tolerable si nota > 7 (encerts > 70%).**
12.4.2 Protecció de dades de prova	Les proves s'executen en entorns segurs (sense accés usuaris).	
12.4.3 Control d'accés al codi font	Només el Departament de Tecnologies de la Informació hi té accés.	
12.5 Seguretat en el desenvolupament i en el suport		
12.5.1 Procediments de control de canvis	Pendent. No existeix un procediment, es generen còpies de modificacions.	Temps d'aplicació de modificacions de seguretat entre aparició de vulnerabilitat, proves, revisió i aplicació final de canvis. **Acceptable per temps menors de 24h.**
12.5.2 Revisió tècnica de canvis en el sistema operatiu	Execució de bateria de proves després d'aplicació de canvis.	
12.5.3 Restricció de canvis en paquets de programari	Actualitzacions manuals a Windows, repositoris de seguretat en Linux.	
12.5.4 Fuites d'informació a través del codi	Revisió de fase de test per part d'analista o programador senior.	
12.5.5 Externalització de desenvolupament de programari	Nagios i monitor de processos, així com l'IDS per detectar anomalies.	Determinació del temps de no disponibilitat de serveis externs. Suma i mitja. **Tolerable per**

		percentatges de disponibilitat majors del 98%.
12.6 Gestió de les vulnerabilitats tècniques		
12.6.1 Control de les vulnerabilitats tècniques	Eina de gestió d'incidències TIC disponible per departament TIC.	Incidències tractades des de l'eina (anualment) del total de rebudes o reportades. **Acceptable si és més del 75%.**
13. GESTIÓ D'INCIDÈNCIES DE SEGURETAT DE LA INFORMACIÓ		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
13.1 Notificació d'incidències i debilitats *		
13.1.1 Notificació d'esdeveniments de seguretat	Configurats canals de correu electrònic i SMS (via módem GSM) per Nagios.	Número de notificacions diàries/setmanals d'incidències i debilitats, tant per SMS com per telèfon. **Acceptable per sota de 5 (de mitja setmanal).**
13.1.2 Notificació de debilitats	Cal formalització en el contracte.	
13.2 Gestió d'incidències i millora *		
13.2.1 Identificació de responsabilitats i procediments	En documents de la Política de la Seguretat estan definits. Faltarien procediments.	Entrevista a personal. Obtenció de mitges. **Tolerable si nota > 7 (encerts > 70%).** Revisió últimes modificacions de política. Número de revisions pel període (anualment). **Acceptable per un mínim de 3 revisions.**
13.2.2 Avaluació d'incidències	Cal crear base de dades de coneixement d'accidents o incidències.	Consulta de 5 incidències anteriors aleatòries. % d'incidències documentades respecte totals. **Tolerable si un mínim d'un 80% de les incidències estan documentades.**
13.2.3 Recol·lecció d'evidències	Dades d'auditoria i registres de log. Cal procediment.	Entrevista i valoració de respostes respecte procediment. **Acceptable si nota > 7 (encerts > 70%).**
14. GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI *		

CONTROL ISO	IMPLEMENTACIÓ	INDICADOR
14.1 Gestió de la continuïtat del negoci		
14.1.1 Procés de gestió de la continuïtat del negoci	S'està realitzant però no està del tot documentat. En procés.	Utilització models de maduresa (CMMI). **Tolerable per sobre de L3.**
14.1.2 Continuïtat de negoci i anàlisi d'impacte	Pendent de realitzar. No implementat.	Revisió últims canvis. Número de canvis realitzats dins període d'estudi. Percentatge de processos de l'organització amb plans de continuïtat documentats i provats durant el període especificat. **Tolerable per % superior a 75%.**
14.1.3 Documentació i implantació del pla de continuïtat	Revisió periòdica per revisió d'elements i processos a tenir en compte.	
14.1.4 Marc de planificació	S'està realitzant però no està del tot documentat. En procés.	
14.1.5 Procés, manteniment i avaluació de Plans de continuïtat	Pendent de realitzar. No implementat.	
15. CONFORMITAT		
CONTROL ISO	**IMPLEMENTACIÓ**	**INDICADOR**
15.1 Conformitat amb requisits legals		
15.1.1 Identificació de la legislació aplicable	Realitzat en aquest document.	Número de recomanacions respecte aspectes legals, agrupades per estat actual (obertes, tancades, en curs) i risc. **Percentatge de tancades respecte les rebudes, tolerable si tancades és superior al 75%.**
15.1.2 Dret de la propietat intel·lectual *	Revisió i compra de les respectives llicències. Cal crear inventari de llicències.	
15.1.3 Control de seguretat de registres de l'organització *	Ho recullen la política de seguretat o els diferents contractes i convenis.	
15.1.4 Protecció dades de caràcter personal i de la intimitat *	L'organització aplica i és auditada per validar la correcta aplicació de la LOPD.	
15.1.5 Evitar mal ús de recursos de tractament de la informació	Utilització de l'IDS o tràfic de Firewall, així com revisió de registres del sistema en cas de sospita.	
15.1.6 Reglamentació de controls de xifratge	L'Ajuntament revisa la legislació i rep notificació dels canvis.	Número d'últims canvis no aplicats. **Percentatge de canvis no aplicats menor d'un 5%.**

15.2 Compliment del marc normatiu		
15.2.1 Compliment de polítiques i normes	Falta de procediments i política fins ara. Es precisarà formació.	Realització d'entrevistes i valoracions. **Acceptable si nota > 7 (encerts > 70%).**
15.2.2 Comprovació de la conformitat tècnica	Pendent, no està implementat.	
15.3 Auditoria de sistemes		
15.3.1 Controls d'auditoria de sistemes	No hi ha cap gestió d'auditories de moment. Cal implementar-la.	Revisió en documentació d'últims registres d'auditoria. **Tolerable si el número de revisions d'auditories últim trimestre major 1.**
15.3.2 Protecció d'eines d'auditoria	Algunes detectades per l'IDS. Accés restringit però cal impossibilitar la descàrrega.	

A1.5 PROCEDIMENT DE REVISIÓ PER DIRECCIÓ

Capçalera:

Codi:	SGSI-PROCS-REVISIO-DIRRECCIO
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	18/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document
-	-	-	-

A1.5.1 INTRODUCCIÓ

La **Junta de Govern Local** de l'Ajuntament de Riberola serà l'encarregada de revisar

periòdicament el Sistema de Gestió de Seguretat de la Informació per tal de comprovar que es segueix adaptant als objectius de l'organització, així com avaluar el seu estat i prendre les decisions necessàries per tal de seguir-lo millorant i desenvolupant.

Aquesta revisió forma part de la fase de *Comprovar* (“*Check*”) del cicle de millora continua (cicle PDCA) que qualsevol Sistema de Gestió de Seguretat de la Informació ha de complir per tal d'adaptar-se a la ISO/IEC 27001.

A1.5.2 PERIODICITAT

La Junta de Govern Local programarà una revisió anual del Sistema de Gestió de Seguretat de la Informació, sempre un cop acabat el procés d'auditoria interna que també es realitza anualment.

A1.5.3 PROCEDIMENT

El Comitè de Seguretat de les Tecnologies de la Informació i la Comunicació serà l'encarregat de proporcionar a la Junta de Govern Local els diferents documents per tal que la aquesta última disposi de la informació necessària per:

a) Conèixer l'estat actual del Sistema de Gestió de Seguretat de la Informació.

b) Tenir coneixement d'estadístiques d'incidències en matèria de seguretat de la informació.

c) Tenir coneixement dels resultats de l'última auditoria interna realitzada.

d) Conèixer la situació dels projectes en matèria de seguretat en curs, així com els possibles a realitzar en un futur.

El Comitè de Seguretat haurà de conèixer amb antelació la data de la sessió en que es realitzarà la revisió per poder aportar la documentació necessària a la Junta de Govern Local.

A1.5.4 DADES D'ENTRADA

La documentació a aportar ha de ser entenedora per part de personal no tècnic ni especialitzat en matèria de seguretat, i no ha de ser poc extensa i específica. La documentació a remetre a la Junta de Govern Local inclourà:

- Auditories portades a terme en l'organització en relació a la seguretat de la informació. Per tant no només s'inclouran els resultats de l'auditoria interna del SGSI, sinó que a més s'incorporaran altres resultats de possibles auditories com poden ser de la Llei Orgànica de Protecció de Dades.
- Anteriors revisions del SGSI i les accions derivades de les mateixes. S'avaluaran les

decisions anteriors preses i es podrà observar fins on s'ha arribat amb aquestes decisions, o si encara en resten de pendents.

- Resum estadístic d'incidències relacionades amb la seguretat i evolució dels últims mesos o anys.
- Proposta per part del Comitè de Seguretat de noves tècniques, procediments o productes que puguin aportar millores de funcionament o efectivitat al SGSI actual.
- Estat de les accions preventives i correctores. Observar quantes se n'han realitzat, temps d'implementació, origen i motiu pot aportar una informació molt valuosa per avaluar l'estat actual del SGSI de l'organització.
- Avaluació dels objectius. Es revisarà si s'estan complint els objectius marcats en un inici.
- Si hi han canvis organitzatius que afectin d'alguna manera la gestió de la informació o dels sistemes relacionats, caldrà indicar-ho per si cal realitzar alguna actuació.

A1.5.5 DADES DE SORTIDA O RESOLUCIÓ

La Junta de Govern Local redactarà un resolució en el qual reflectirà les possibles observacions, idees, raonaments o decisions respecte l'estat actual o futur del Sistema de Gestió de la Informació de l'Ajuntament de Riberola.

En el cas que la Junta de Govern Local observi algun punt desfavorable o aspecte important a millorar, caldrà que aparegui en la resolució esmentada per a que el Comitè de Seguretat en tingui constància i es reflecteixi en la documentació del mateix SGSI.

Per tant, de la revisió en sorgirà una documentació que quedarà registrada al SGSI i que pot incloure:

- Millores a implementar en el SGSI, si s'escau.
- Actualització de l'avaluació i gestió de riscos, si s'escau.
- Modificació de procediments i controls que afecten la seguretat de la informació, si s'escauen. Poden venir provocats per:
    - Nous requeriments de seguretat o legals.
    - Obligacions contractuals (nous convenis o contractes).
    - Canvis en els nivells de risc acceptable.
    - Necessitats de recursos.

- Millores en la manera de mesurar l'efectivitat dels controls. Al revisar els indicadors i les mètriques cal avaluar si segueixen sent útils o cal eliminar-los o substituir-los per altres.

A1.5.6 ALTRES CONSIDERACIONS

- La Junta de Govern Local té la capacitat de requerir una revisió del SGSI quan així ho sol·liciti. El Comitè de Seguretat disposarà de quinze dies per a preparar la documentació necessària per poder-la remetre a la Junta de Govern Local.
- En cas que la Junta de Govern Local observi anomalies o sorgeixin molts dubtes durant la revisió, es podrà sol·licitar la presència d'un o més membres del Comitè de Seguretat per tal de completar certa informació o resoldre possibles dubtes en una sessió posterior. La resolució d'aquesta sessió posterior també serà registrada dins el SGSI.

A1.6 GESTIÓ DE ROLS I RESPONSABILITATS

Capçalera:

Codi:	SGSI-PROCS-ROLS-RESPONS
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	18/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
18/03/2013	0.1	Ricard Salvat	Creació del document
-	-	-	-

A1.6.1 INTRODUCCIÓ

Tal i com es detalla en la Política de Seguretat de l'Ajuntament de Riberola, el màxim responsable de l'organització serà la Junta de Govern Local.

En matèria de seguretat, la Junta de Govern Local nomenarà el Comitè de Seguretat de

Tecnologies de la Informació i la Comunicació. Aquest comitè serà l'encarregat de proposar el càrrec de Responsable de Seguretat a la Junta, per la seva aprovació.

Així mateix, l'organització es divideix en departaments, els quals disposen d'un responsable o cap de departament. La resta del personal es divideix en tècnics i administratius o auxiliars administratius. La major part del personal té accés als sistemes informàtics que proporciona l'Ajuntament als seus treballadors per tal de realitzar les seves tasques assignades.

A1.6.2 ESTRUCTURA ORGANITZATIVA

L'estructura de l'organització en matèria de seguretat de la informació estarà dividida en tres nivells de manera jeràrquica: estratègic, tàctic i operatiu (*Figura 6-1*).

La Junta de Govern Local es troba en el nivell estratègic, ja que aporta els recursos necessaris i la visió estratègica de conjunt de l'organització.

El Comitè de Seguretat estarà entre el nivell estratègic i el nivell tàctic. Estarà composat per:

- Responsable de Seguretat (també forma part del Departament de Tecnologies de la Informació i la Comunicació).
- Regidor de Tecnologies de la Informació i Comunicació (també forma part de la Junta de Govern Local).
- Departament de Tecnologies de la Informació i Comunicació.
- Cap d'Organització o Recursos Humans.
- Cap de l'Oficina d'Atenció al Ciutadà.

Addicionalment el Comitè de Seguretat podrà convidar a les seves sessions a qui cregui oportú o necessari convocar.

El Responsable de Seguretat de la informació formarà part del nivell tàctic, aportant la gestió i coordinació en matèria de seguretat. En controlarà els processos i n'informarà al Comitè de Seguretat.

Finalment, l'últim nivell seria l'operatiu, del qual en formen part els diferents departaments municipals, incloent el de Tecnologies de la Informació i la Comunicació.

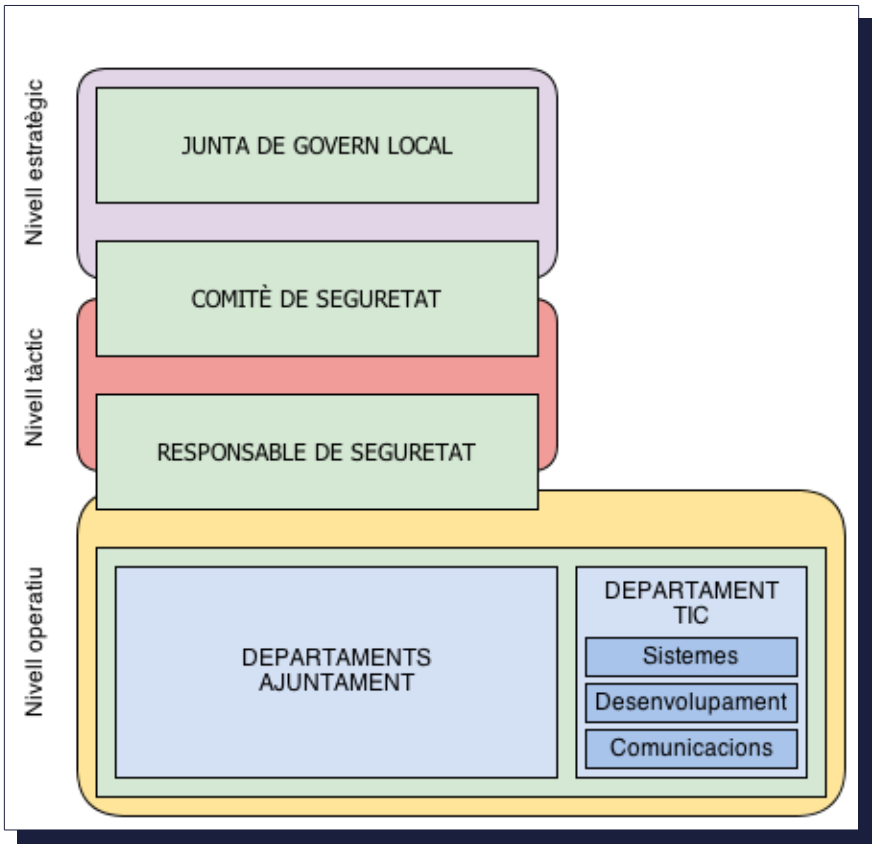

Figura A1-6-1: Estructura organitzativa en seguretat.

A1.6.3 ROLS

Respecte la informació, podem distingir tres rols molt clars: propietari, administrador i usuari.

Considerant la major part dels treballadors, es considerarà que els propietaris de la informació seran els caps dels diferents departaments, així com els regidors de cadascuna de les àrees. El rol d'administrador recaurà sobre el personal del Departament de Tecnologies de la Informació i la Comunicació, ja que són els qui administren els sistemes en els que s'emmagatzema i es tracta tota la informació. Finalment el rol d'usuaris recaurà sobre tots els treballadors que utilitzen els serveis de l'Ajuntament.

A1.6.4 RESPONSABILITATS

Les responsabilitats de la Junta de Govern Local en matèria de seguretat, les del Comitè de Seguretat i les del Responsable de Seguretat estan establertes en la Política de Seguretat de l'Ajuntament de Riberola.

D'altra banda, en la següent llista es presenten les responsabilitats per cadascun dels rols definits en l'apartat anterior:

a) Propietaris

Els propietaris de la informació seran els encarregats de definir, respecte la informació que gestionen:

- Grau de confidencialitat de la informació.
- Drets d'accés.
- Formes d'explotació de la informació.

b) Administradors

Els administradors tenen dret a la major part de la informació dels diferents departaments per poder-ne realitzar la seva gestió segons les necessitats dels seus propietaris.

Els seus deures són:

- Administrar els sistemes que contenen i tracten la informació.
- Salvaguardar la informació.
- Implementar els sistemes de control d'accés pertinents.
- Realitzar tasques de còpies de seguretat de les dades.
- Operar i mantenir les mesures de seguretat establertes pels propietaris.

c) Usuaris

Correspon als usuaris el fet de responsabilitzar-se i complir amb tota la normativa vigent de l'organització, procediments i estàndards relacionats amb la seguretat de la informació.

Qüestions que puguin sorgir referents a la gestió apropiada per algun tipus concret d'informació seran dirigides al propietari de la informació (cap de departament) o als administradors pertinents.

Tota la informació que es tracta o es genera a l'Ajuntament de Riberola ha de ser protegida segons el seu nivell de confidencialitat. S'ha de fer ús de mesures de seguretat per protegir la confidencialitat de la informació independentment del suport en el qual s'emmagatzemi la informació (digital, paper, etc.)., sistema en que es processi o mitjà pel qual es retransmeteixi.

A1.7 DECLARACIÓ D'APLICABILITAT

Capçalera:

Codi:	SGSI-DECLAR-APLICABILITAT
Versió:	0.1
Autor:	Ricard Salvat
Revisió:	-
Data de publicació:	21/03/2013
Aprovat per:	Junta de Govern Local
Data d'aprovació:	-
Nivell de confidencialitat:	Normal

Historial de modificacions:

Data	Versió	Creat per	Descripció
21/03/2013	0.1	Ricard Salvat	Creació del document
-	-	-	-

Declaració d'aplicabilitat:

5. POLÍTICA DE SEGURETAT			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
5.1 Política de seguretat de la informació			
5.1.1 Document de política de seguretat *	SI	Control necessari per la norma ISO, política seguretat de l'empresa. Conté polítiques d'alt nivell i cal que tothom les conegui.	Pendent de revisió i aprovació per JGL. Proposta adjunta en projecte TFM.
5.1.2 Revisió de la política de seguretat	SI	Cal revisió periòdica per aplicar modificacions i revisió objectius.	Establiment periodicitat de revisió/aprovació.
6. ORGANITZACIÓ DE LA SEGURETAT DE LA INFORMACIÓ			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
6.1 Organització interna			
6.1.1 Comitè de seguretat	SI	Per mida d'organització, es	Pendent de

		requereix comitè de seguretat com a rol entre JGL i responsable de seguretat. Elevació propostes a JGL (direcció).	formació. Documentat en proposta en projecte TFM.
6.1.2 Coordinació	SI	És necessària una coordinació en matèria de seguretat per tal de gestionar el SGSI de l'empresa i que vagi evolucionant amb el cicle continu PDCA.	En la definició de rols i funcions proposada en aquest TFM hi ha una proposta. Cal revisió i aprovació.
6.1.3 Assignació de responsabilitats *	SI	Tot i que existeixen certes assignacions de funcions, cal un document que les especifiqui. Control essencial de la ISO.	Definició formal en document actual. Cal revisió i aprovació.
6.1.4 Autorització de recursos	SI	Cal un procediment per la sol·licitud de nous processos o accessos a recursos / informació.	Pendent de realitzar. Cal que existeixi el document pertinent.
6.1.5 Acords de confidencialitat	SI	Qualsevol contracte o conveni ha de contenir clàusules de confidencialitat per les dades tractades.	Al ser administració pública tots els serveis van regulats per convenis o contractes.
6.1.6 Contacte amb autoritats	SI	Cal disposar de contactes amb autoritats i organismes competents en cas d'incidents de seguretat o detecció d'activitats compromeses.	Implementat. Procediment Policia local – Mossos d'esquadra. Contactes INTECO i CESICAT.
6.1.7 Contacte amb altres grups d'interès	SI	Intercanvi de coneixements, notícies i obtenció de serveis de seguretat.	L'organització està en llistes de INTECO-CERT i CESICAT, entre altres.
6.1.8 Revisió independent	SI	Cal una revisió o auditoria interna realitzada per una empresa o	No es preveu pròximament. Cal

		personal extern per tal de validar els processos i informació del SGSI.	contractar empresa externa per auditoria / revisió del SGSI.
6.2 Tercers			
6.2.1 Identificació de recursos	SI	Existeixen certes aplicacions crítiques dins el sistema que estan desenvolupades per empreses externes, així com alguns processos amb altres administracions.	Subconjunt de l'inventari d'actius, serveis gestionats per empreses externes.
6.2.2 Seguretat en la relació amb clients	SI	La ciutadania ha de veure garantida els seus drets segons regula la Llei Orgànica de Protecció de Dades.	Aplica la LOPD per la relació amb els clients, en el nostre cas la ciutadania.
6.2.3 Seguretat en acords amb terceres parts	SI	Existeixen contractes de serveis amb tercers.	En cas de serveis TIC, sempre es preveuen els punts de seguretat en els diferents contractes.
7. GESTIÓ D'ACTIUS			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
7.1 Responsabilitats sobre els actius			
7.1.1 Inventari d'actius	SI	Cal realitzar un inventari dels actius per poder-ne realitzar la gestió apropiada.	Mitjançant Magerit. Identificació d'actius present en aquest document.
7.1.2 Propietat dels actius	SI	Tots els actius cal que disposin d'un propietari dins l'organització.	En la documentació dels actius ha de constar el propietari(s).
7.1.3 Ús acceptable dels actius	SI	Informar al personal de l'organització dels drets i deures de la utilització dels actius.	Generació de documents de polítiques d'ús (i aplicació).

			Polítiques en Active Directory, Tallafocs i Proxy.
7.2 Classificació de la Informació			
7.2.1 Guies de classificació	SI	Cal classificar la informació per tal de poder aplicar criteris legals com la LOPD.	Acció realitzada per adaptació a la LOPD. Consultar Document de Seguretat.
7.2.2 Marcatge i tractament de la informació	SI	Cal realitzar un marcatge de la informació per tal de saber-ne la seva classificació. Evita possibles fugues d'informació.	La informació es tracta actualment segons classificació. Pendent etiquetar.
8. SEGURETAT RELATIVA AL PERSONAL			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
8.1 Abans de la contractació			
8.1.1 Rols i responsabilitats	SI	És necessari que els futurs empleats i empreses externes coneguin amb antelació les responsabilitats i polítiques sota les que hauran de realitzar les seves activitats.	Comunicació de polítiques de seguretat en paper i versió electrònica a candidats i empreses.
8.1.2 Selecció i política de personal	SI	Verificació de les dades aportades per particulars i empreses.	Al ser administració pública es realitzen les verificacions pertinents, siguin processos d'empreses o particulars.
8.1.3 Termes i condicions de la relació laboral	SI	Cal assegurar-se que se segueixin les polítiques de manera formal.	Introducció en el contracte de clàusula d'acceptació de polítiques de seguretat.
8.2 Durant la relació laboral			

8.2.1 Supervisió d'obligacions	SI	Direcció ha de requerir als empleats i empreses externes que segueixin les polítiques definides.	Signatura de clàusula en contractes i convenis.
8.2.2 Conscienciació, formació i capacitació en seguretat *	SI	Cal realitzar formació de seguretat de manera periòdica al personal de l'Ajuntament.	Es precisa de planificació periòdica de formació. Dotació de pressupost anual.
8.2.3 Procediment disciplinari	SI	Ha d'existir un procés disciplinari en cas d'empleats o tercers que realitzin activitats il·lícites en matèria de seguretat de la informació.	Està formalitzat en les bases de l'administració local.
8.3 En finalitzar la contractació o canvi d'ocupació			
8.3.1 Cessació de responsabilitats	SI	Cal un procediment en la cessació de responsabilitats d'un empleat.	Existeix, però no està documentat actualment.
8.3.2 Devolució d'actius	SI	S'ha de sol·licitar la devolució de tots els actius propietat de l'organització.	Document signat conforme se li proporciona, i que cal tornar-lo un cop finalitzada l'activitat.
8.3.3 Eliminació de drets d'accés	SI	Cal eliminar tots els drets d'accés físics i lògics de la persona o entitat que finalitza contracte.	Personal comunica baixes en correu electrònic a Responsable de seguretat.
9. SEGURETAT FÍSICA I DE L'ENTORN			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
9.1 Àrees segures			
9.1.1 Perímetre de	SI	Es precisa prevenir l'accés no	Es disposa d'accés

seguretat física		autoritzat a zones que disposen d'accés a la informació.	autenticat amb codi, taulells de recepció i portes amb pany (clau) en les diferents dependències.
9.1.2 Control d'accés físic	SI	Les zones més importants com Centres de Processament de Dades precisen d'un control d'accés.	Els tres CPD estan darrera de portes tancades amb clau.
9.1.3 Seguretat en oficines, despatxos i recursos	SI	Cal controlar els accessos no autoritzats a zones on es tracta informació confidencial.	Presència de gent constant i dispositius de perímetre punt 9.1.1 per fora horari.
9.1.4 Protecció enfront d'amenaces externes i d'entorn	SI	Control de foc, inundacions i altres desastres externs.	Existència d'extintors de diferents tipus segons actius propers.
9.1.5 El treball en àrees segures	No	No existeixen àrees de seguretat especial de tipus químic o electromagnètic.	No es requeriex.
9.1.6 Accés públic, zones de càrrega i descàrrega	No	No existeixen àrees de càrrega i descàrrega específiques que afectin els actius TIC.	No es requeriex.
9.2 Seguretat en equips			
9.2.1 Ubicació i protecció	SI	Els equipaments i altres elements han d'estar degudament situats i protegits per evitar accessos indeguts o incidents.	Protecció de servidors i commutadors dins armaris RACK. Cal procediment per estacions de treball i altres elements menys

			crítics.
9.2.2 Subministraments	SI	Subministrament elèctric addicional necessari per mantenir serveis i electrònica de xarxa, així com un mínim d'estacions de treball per no perdre disponibilitat de serveis davant el ciutadà.	Els CPD disposen de SAIs. Pendent SAI per un mínim d'estacions de treball.
9.2.3 Seguretat del cablejat	SI	És necessari evitar possibles talls de connexió o intercepcions de tràfic de dades en mitjan de telecomunicació.	Desplegament de cablejat ethernet en paret i fibra òptica en rasa sempre que sigui possible.
9.2.4 Manteniment dels equips	SI	Realització periòdica de tasques de manteniment en els actius per mantenir disponibilitat i integritat.	Es disposa de contractes de manteniment en serveis centrals. Tasques menors en altres elements.
9.2.5 Seguretat fora dels locals	SI	Cal prendre mesures de seguretat en equips que treballen fora de les dependències municipals.	Portàtils, memòries USB i telèfons amb codis d'accés i si és possible, partició xifrada de dades per emmagatzemar informació.
9.2.6 Reutilització o eliminació	SI	En cas de substitució d'equipament o eliminació, cal procedir a eliminació segura de rastre de dades.	Contractació d'empresa externa puntualment per destrucció d'elements presumibles de contenir dades.
9.2.7 Autorització de sortida	SI	L'equipament i la informació de l'organització no hauria de sortir	No existeix actualment cap

		sense la pertinent autorització signada.	procediment similar. Cal redactar, revisar i aprovar el document.
10. GESTIÓ DE COMUNICACIONS I OPERACIONS			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
10.1 Procediments d'operació i responsabilitats			
10.1.1 Documentació de procediments	SI	Els diferents procediments de l'organització per documentar els processos han d'existir i ser accessibles a qui ho necessiti.	Pendent d'implementar en la major part de departaments. Cal eina (p.ex. Wiki) i redacció de procediments.
10.1.2 Gestió de canvis	SI	Es precisa d'un gestor de canvis per documents compartits i les seves versions, així com desenvolupaments del departament TIC.	Eina de gestió documental i GIT o similar pendents d'implementar.
10.1.3 Segregació de funcions	SI	Han d'existir diferents funcions en diferents departaments per evitar modificacions perjudicials, intencionades o no.	Existeixen diferents nivells de treballadors segons les seves funcions en cada departament. Consta en contracte.
10.1.4 Separació d'entorns desenvolupament i producció	SI	Cal que existeixi un entorn de desenvolupament on provar nous productes o desenvolupaments sense afectar l'entorn de producció i la seva disponibilitat.	En l'àrea TIC es disposa de maquinari preparat per realitzar d'entorn de proves.
10.2 Gestió de la prestació de serveis per tercers			
10.2.1 Prestació de serveis	SI	Cal assegurar-se que els controls de seguretat, definicions de	Sol·licitar informació

		serveis i nivells de disponibilitat i entrega són executats correctament pels tercers.	periòdicament per part del Responsable de Seguretat.
10.2.2 Monitoratge i revisió de serveis	SI	Els serveis oferts per tercers a l'organització han de ser controlats i revisats de manera periòdica.	S'utilitza l'eina Nagios per controlar els serveis i elements TIC.
10.2.3 Gestió de canvis en els serveis	SI	Cal un procediment per la realització de canvis en els serveis oferts per tercers.	Còpia de dades involucrades, execució fora hores d'atenció i en cas de canvi crític, proves en entorn de proves.
10.3 Planificació i acceptació del sistema			
10.3.1 Gestió de la capacitat	SI	S'ha de controlar l'ús dels recursos actuals per assegurar un bon rendiment del sistema.	Nagios, VMWare i OSSIM IDS permeten la monitorització i control d'aquests recursos i serveis.
10.3.2 Acceptació de sistemes	SI	Només s'aplicarà un canvi a producció quan estigui degudament provat.	No s'actualitza res dels diferents sistemes fins que el departament TIC no ho aprova.
10.4 Protecció conta codi maliciós			
10.4.1 Protecció contra codi maliciós	SI	Cal protegir els sistemes de virus i codi maliciós per mantenir integritat, disponibilitat i confidencialitat.	Es disposa d'antivirus, proxy, firewall i programa anti-malware i IDS. Cal canviar algun sistema antic.
10.4.2 Protecció contra codi descarregat en el client	SI	Protecció d'execucions de programes en estacions de treball, un cop descarregada	Control tràfic de xarxa (IDS), a més de permisos limitats

		aplicació maliciosa o no acceptada per política.	en estacions de treball per evitar instal·lacions de programari no autoritzat.
10.5 Gestió de suports i recuperació			
10.5.1 Recuperació de la informació	SI	S'ha de poder recuperar informació extraviada o alterada de manera accidental si és necessari, dins d'un període de 15 dies.	Sistema de còpies de seguretat en cinta, fins a 25 dies d'antiguitat.
10.6 Gestió de la seguretat de xarxes			
10.6.1 Controls de xarxa	SI	Cal controlar els accessos a la xarxa, a Internet i des d'Internet, així com als servidors i entre estacions de treball.	Existència de Tallafocs, Proxy i control de tràfic per IDS (Snort – OSSIM).
10.6.2 Seguretat dels serveis de xarxa	SI	Els serveis de xarxa s'han d'administrar de manera segura, són la base de les comunicacions.	Separació de xarxes i creació de subxarxes. Control de serveis per Nagios.
10.7 Gestió de suports d'informació			
10.7.1 Gestió de suports extraïbles	SI	Cal que existeixi un procediment a l'abast dels usuaris per tal de gestionar els suports extraïbles de manera segura.	Pendent. A incloure en futura wiki de seguretat.
10.7.2 Retirada de suports	SI	Eliminació segura de possibles dades en el procés de retirada de suport.	Eliminació per empresa externa autoritzada i certificada. Igual que en control 9.2.6.
10.7.3 Procediments d'utilització de la informació	SI	Cal que existeixi un procediment a l'abast dels usuaris per tal de tractar i emmagatzemar la informació.	Pendent. A incloure en futura wiki de seguretat.

10.7.4 Seguretat en la documentació dels sistemes	SI	Ha d'existir protecció a un accés no autoritzat per accedir a documentació dels sistemes de l'Ajuntament.	S'emmagatzema en digital, amb restriccions d'accés i en caixa forta de manera física.
10.8 Intercanvi d'informació			
10.8.1 Polítiques i procediments d'intercanvi d'informació	SI	Existeixen intercanvis d'informació, però cal documentar-los i emmagatzemar-los de manera segura.	Pendent, ja que existeixen però no queden degudament documentats.
10.8.2 Acords d'intercanvi	SI	Cal garantir formalment la seguretat de les dades en processos d'intercanvi amb altres entitats o administracions.	Sempre hi ha una signatura de conveni o contracte on es contemplen aquest tipus de clàusules.
10.8.3 Suports físics en trànsit	SI	Les dades que van en suports físics en trànsit han d'estar degudament protegides.	Pendent de realitzar procediment. Actualment no es xifren ni es comprova l'autenticitat.
10.8.4 Missatgeria electrònica	SI	Cal assegurar el correu electrònic i les comunicacions d'aquest cap a Internet.	El servidor disposa d'antivirus i antispam. Les comunicacions requereixen protocol SSL xifrat.
10.8.5 Sistemes d'informació del negoci	SI	Els procediments i polítiques de l'empresa han d'estar degudament alineats amb les polítiques de seguretat.	Revisió periòdica de procediments i sistemàtica en canvi de flux de treball.
10.9 Serveis de comerç electrònic			
10.9.1 Comerç electrònic	No	No es disposa de l'opció de comerç electrònic més enllà d'enllaçar	No es requereix.

		amb entitat bancària.	
10.9.2 Transaccions en línia	No	No es realitzen transaccions en línia més enllà d'enllaçar amb entitat bancària.	No es requereix.
10.9.3 Informació d'accés públic	SI	El ciutadà ha de poder mantenir els seus drets de protecció de dades personals.	Es segueix la LOPD en els diferents processos de l'Ajuntament relacionats amb ciutadans.
10.10 Monitoratge			
10.10.1 Registre d'activitats	SI	Emmagatzemar un registre de les activitats i errors dels usuaris en els sistemes.	Els realitza, però caldria incrementar nivell de detall.
10.10.2 Ús dels sistemes de monitoratge	SI	Procediment de monitoratge de sistemes documentat. Serveix per preveure errors i reduir el temps de resolució d'incidències.	Els sistemes de procés d'informació estan monitoritzats per Nagios i VMWare. Cal documentar.
10.10.3 Protecció de les traces i registres	SI	Els registres existents cal que siguin protegits per tal de evitar la seva manipulació o modificació malintencionada.	El
10.10.4 Traces d'administració i operació	SI	Les accions d'operació i administració han de ser correctament registrades.	Habilitar registres d'auditoria en servidors per qualsevol usuari.
10.10.5 Registre de fallades	SI	Es precisa d'un registre d'errors de sistemes per poder avaluar el seu estat.	Registres d'error habilitats en el servidor.
10.10.6 Sincronització de rellotges	SI	Els diferents serveis i elements han d'interactuar amb l'hora correcta.	Utilització de protocol de xarxa NTP.
11. CONTROL D'ACCÉS			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**

11.1 Requisits de negoci pel control d'accés			
11.1.1 Política de control d'accés	SI	Es desitja un control d'accés als recursos d'informació de l'organització.	Implementat mitjançant comptes Active Directory.
11.2 Gestió d'accés dels usuaris			
11.2.1 Registre d'usuaris	SI	Es requereix un procediment formal per registrar i eliminar un usuari dels sistemes i dels accessos.	Operació realitzable amb Active Directory.
11.2.2 Gestió de privilegis	SI	Els usuaris han de disposar d'un sistema de privilegis al accedir al sistema o a la informació.	Divisió d'usuaris en grups per assignació de permisos. Drets d'operacions respecte grups o usuaris amb AD.
11.2.3 Gestió de contrasenyes d'usuari	SI	Cal gestionar les claus d'accés dels diferents usuaris del sistema.	Gestió des d'Active Directory.
11.2.4 Revisió dels drets d'accés d'usuari	SI	Es necessita un procediment per establir una revisió periòdica dels drets d'accés actuals.	Tasca a realitzar, cal assignar periodicitat i documentar.
11.3 Responsabilitat dels usuaris			
11.3.1 Ús de credencials	SI	Cal requerir als usuaris que utilitzin bones pràctiques en la selecció de paraules de pas.	Forçat per política AD.
11.3.2 Equips d'usuaris desatesos	SI	Es requereix el bloqueig de la pantalla en temps d'inactivitat.	Política AD. Bloquejar en 20 minuts d'inactivitat.
11.3.3 Política de taules i pantalles netes	SI	Cal adoptar una política de taules sense papers ni mitjans extraïbles, i pantalles netes.	Falta redactar i adoptar política per part de personal.
11.4 Control d'accés a la xarxa			
11.4.1 Política d'ús dels serveis de la xarxa	SI	Només usuaris habilitats poden accedir als recursos de xarxa.	Autenticació d'usuari en AD directament o per LDAP (Linux).

11.4.2 Autenticació d'usuaris per a connexions remotes	SI	Accés d'usuaris en serveis des de connexió remota requereix autenticació.	Autenticació d'usuari per LDAP (Linux).
11.4.3 Autenticació de nodes a la xarxa	SI	Es requereix autenticació d'equip per tal d'accedir a la xarxa, no només d'usuari.	Configurat en Active Directory.
11.4.4 Protecció dels ports de diagnòstic i configuració remots	SI	Control d'accessos remots.	Control de firewall, registres del IDS i controls periòdics exteriors per CESICAT.
11.4.5 Segregació de les xarxes	SI	Xarxes de Veu IP, administració de xarxa, dades i Internet pública separades.	Són tot xarxes independents, habilitades per VLAN, tallafocs i routers.
11.4.6 Control de la connexió a la xarxa	SI	Cal controlar les possibilitats de connexió dels diferents usuaris a la xarxa de l'organització.	Active directory permet assignar horaris i estacions permeses a usuaris concrets. Pendent millorar les restriccions.
11.4.7 Control d'encaminament a la xarxa	SI	Cal controlar l'accés del tràfic de la xarxa i el seu flux.	Routers i tallafocs. IDS per registrar anomalies.
11.5 Control d'accés al sistema operatiu			
11.5.1 Procediments de connexió segur	SI	Cal un procés d'autenticació d'usuaris segur i confiable.	Accés autenticat segur amb AD o LDAP amb SSL.
11.5.2 Identificació i autenticació d'usuaris	SI	Identificador únic per usuari, intransferible.	Implementat en AD, existència d'algun usuari genèric per alguna tasca residual.
11.5.3 Sistema de gestió	SI	Cal aplicar polítiques restrictives	Pendent

de contrasenyes		de contrasenyes i que l'usuari la pugui canviar quan desitgi.	incrementar polítiques de contrasenyes i habilitació de canvi.
11.5.4 Ús dels serveis del sistema	SI	L'accés als serveis oferts ha de ser sota els permisos d'accés correctes.	Sempre es requereix algun tipus d'autenticació.
11.5.5 Desconnexió automàtica de sessió	SI	Tancar sessions amb període d'inactivitat superior a 15 min.	Actualment algun servei no ho realitza. Cal forçar-ho (aplicació padró i expedients)
11.5.6 Limitació del temps de connexió	SI	En connexions d'alt risc (com per exemple Terminal Servers a Servidors) cal un temps màxim abans de desconnexió.	Està habilitat en la major part de servidors. Revisar i configurar la resta.
11.6 Control d'accés a la informació i a les aplicacions			
11.6.1 Restricció d'accés a la informació	SI	Restringir accés a dades i aplicacions segons usuari i polítiques d'accés.	Implementat per AD.
11.6.2 Aïllament de sistemes sensibles	SI	Cal aïllar els sistemes sensibles (aplicacions crítiques) per disminuir risc i augmentar rendiments i seguretat.	Dos servidors Windows 2003 suporten les dos principals aplicacions de l'organització.
11.7 Informàtica mòbil i teletreball			
11.7.1 Informàtica mòbil i comunicacions	SI	Cal crear una política d'ús d'aparells de telefonia mòbil i formar els usuaris.	Pendent realitzar el procediment. Actualment formació puntual en entrega de terminal.
11.7.2 Teletreball	No	No existeixen casos dins l'organització ni es permet per part de direcció.	No es requereix.

12. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DE SISTEMES D'INFORMACIÓ			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
12.1 Requisits de seguretat en sistemes d'informació			
12.1.1 Anàlisi i especificació de requisits	SI	Els requeriments i especificacions de nous sistemes cal que requereixin els requeriments de controls de seguretat.	Adjunt en documentació de requeriments.
12.2 Control de processos en aplicacions			
12.2.1 Validació de dades d'entrada	SI	Validació de dades d'entrada en cas d'aplicacions on interactua l'usuari.	Es realitza sempre en la mateixa aplicació, segons tipus de dades a introduir.
12.2.2 Control de processos interns	SI	Introducció de processos de validació per comprovar integritat de les dades per controlar errors o manipulacions de les dades.	No s'està realitzant. Cal realitzar-los segons aplicació.
12.2.3 Integritat de missatges	SI	Control d'autenticitat i integritat dels missatges intercanviats entre aplicacions.	Procés de verificació en procés de dades automàtic, segons aplicació.
12.2.4 Validació de dades de sortida	SI	En determinats processos cal una validació de les dades de sortida.	En aquests processos, es realitza un enviament de correu electrònic amb sortida de la validació.
12.3 Controls criptogràfics			
12.3.1 Política d'ús de controls criptogràfics	SI	Utilització de certificats o tokens per realitzar signatures d'informació i enviaments xifrats.	Proveïts per CatCERT, certs usuaris en disposen. Cal amplificar-ne l'ús.

12.3.2 Xifratge	SI	Es requereix comunicació xifrada en enviaments de dades cap a l'exterior o des de l'exterior.	Ús de SSL i certificats en certs protocols i serveis.
12.4 Seguretat dels fitxers de sistema			
12.4.1 Control de programari en producció	SI	Cal tenir un procediment per controlar instal·lació de programari que actualment es troba en producció.	Només permès per administradors. Cal crear procediment tot i que es segueixen pautes concretes.
12.4.2 Protecció de dades de prova	SI	L'accés als servidors de prova ha d'estar limitat pels usuaris que ho necessitin únicament i les dades han de ser seleccionades amb cura.	Les proves s'executen en entorns segurs (sense accés usuaris).
12.4.3 Control d'accés al codi font	SI	Cal protegir el codi font dels desenvolupaments d'accessos no autoritzats.	Només el Departament de Tecnologies de la Informació hi té accés.
12.5 Seguretat en el desenvolupament i en el suport			
12.5.1 Procediments de control de canvis	SI	Cal crear procediments de control de canvis per poder gestionar diferents versions de les mateixes aplicacions sense perdre dades i el control d'aquestes modificacions.	Pendent. No existeix un procediment, es generen còpies de modificacions.
12.5.2 Revisió tècnica de canvis en el sistema operatiu	SI	Cal realitzar proves dels serveis un s'actualitzen o canvien certs parts del sistema.	Execució de bateria de proves després d'aplicació de canvis.
12.5.3 Restricció de canvis en paquets de programari	SI	Limitar els canvis i actualitzacions a temes de seguretat, per no desestabilitzar el sistema.	Actualitzacions manuals a Windows, repositoris de seguretat en Linux.
12.5.4 Fuites d'informació	SI	Cal evitar fuites d'informació per	Revisió de fase de

a través del codi		culpa de codi mal escrit o poc controlat.	test per part d'analista o programador senior.
12.5.5 Externalització de desenvolupament de programari	SI	Cal supervisar i monitoritzar les aplicacions que ofereixen empreses externes.	Nagios i monitor de processos, així com l'IDS per detectar anomalies.
12.6 Gestió de les vulnerabilitats tècniques			
12.6.1 Control de les vulnerabilitats tècniques	SI	Control de vulnerabilitats tècniques que van succeint per tractar-les i proporcionar les mesures necessàries per evitar-les.	Eina de gestió d'incidències TIC disponible per departament TIC.
13. GESTIÓ D'INCIDÈNCIES DE SEGURETAT DE LA INFORMACIÓ			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
13.1 Notificació d'incidències i debilitats *			
13.1.1 Notificació d'esdeveniments de seguretat	SI	Cal notificar per diferents canals incidències greus que s'hagin monitoritzat o observat.	Configurats canals de correu electrònic i SMS (via módem GSM) per Nagios.
13.1.2 Notificació de debilitats	SI	Qualsevol empleat o empresa vinculada ha de tenir el deure d'avisar en cas de detecció de debilitat de seguretat alguna mesura o procés.	Cal formalització en el contracte.
13.2 Gestió d'incidències i millora *			
13.2.1 Identificació de responsabilitats i procediments	SI	Assignació de responsabilitats en la gestió de les incidències, així com procediments a seguir segons incidència.	En documents de la Política de la Seguretat estan definits. Faltarien procediments.
13.2.2 Avaluació d'incidències	SI	Fan falta mecanismes per a emmagatzemar i quantificar els diferents accidents succeïts al sistema.	Cal crear base de dades de coneixement d'accidents o

			incidències.
13.2.3 Recol·lecció d'evidències	SI	Cal recollir evidències en cas d'accident de seguretat per tal d'establir responsabilitats i poder presentar les proves necessàries.	Dades d'auditoria i registres de log. Cal procediment.
14. GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI *			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
14.1 Gestió de la continuïtat del negoci			
14.1.1 Procés de gestió de la continuïtat del negoci	SI	Cal l'existència d'un procés que gestioni la continuïtat del negoci, marcant els requeriments per aquesta continuïtat.	Actualment ho realitza el Departament TIC, sense documentació.
14.1.2 Continuïtat de negoci i anàlisi d'impacte	SI	Cal identificar els actius que poden provocar un impacte suficient com per afectar la continuïtat de l'activitat.	Es realitza l'estudi i documentació en el present treball.
14.1.3 Documentació i implantació del pla de continuïtat	SI	Cal documentar els plans de continuïtat tenint en compte diferents causes, per tal d'assegurar uns temps i incidència mínima per restablir el sistema.	S'està realitzant però no està del tot documentat. En procés.
14.1.4 Marc de planificació	SI	Cal un marc únit de planificació de continuïtat per tota l'organització, per assegurar la consistència dels plans i identificar prioritats.	Pendent de realitzar. No implementat.
14.1.5 Procés, manteniment i avaluació de Plans de continuïtat	SI	Cal revisar i actualitzar els plans de continuïtat de manera periòdica.	Revisió periòdica per revisió d'elements i processos a tenir en compte.
15. CONFORMITAT			
CONTROL ISO	**APLICA**	**MOTIUS**	**IMPLEMENTACIÓ**
15.1 Conformitat amb requisits legals			

15.1.1 Identificació de la legislació aplicable	SI	Cal identificar tota la legislació aplicable actualment al respecte.	Realitzat en aquest document.
15.1.2 Dret de la propietat intel·lectual *	SI	Requeriment essencial de la ISO. Inventari de llicències per gestionar la propietat intel·lectual.	Revisió i compra de les respectives llicències. Cal crear inventari de llicències.
15.1.3 Control de seguretat de registres de l'organització *	SI	Els registres i dades importants cal que siguin protegits de pèrdua, destrucció, mitjançant regulació contractual i requeriments de l'organització.	Ho recullen la política de seguretat o els diferents contractes i convenis.
15.1.4 Protecció dades de caràcter personal i de la intimitat *	SI	Cal fer-ho per llei. Essencial a més per la ISO.	L'organització aplica i és auditada per validar la correcta aplicació de la LOPD.
15.1.5 Evitar mal ús de recursos de tractament de la informació	SI	No s'hauria de permetre als usuaris fer ús d'elements de tractament d'informació per usos no autoritzats	Utilització de l'IDS o tràfic de Firewall, així com revisió de registres del sistema en cas de sospita.
15.1.6 Reglamentació de controls de xifratge	SI	Els elements criptogràfics han de ser utilitzats sota la legislació vigent.	L'Ajuntament revisa la legislació i rep notificació dels canvis.
15.2 Compliment del marc normatiu			
15.2.1 Compliment de polítiques i normes	SI	Direcció i caps de departament han de propiciar i forçar el compliment de les normes i procediments.	Falta de procediments i política fins ara. Es precisarà formació.
15.2.2 Comprovació de la conformitat tècnica	SI	Els sistemes d'informació caldrà que siguin comprovats periòdicament per revisar les polítiques i normes.	Pendent, no està implementat.

15.3 Auditoria de sistemes			
15.3.1 Controls d'auditoria de sistemes	SI	Cal una gestió d'auditories, ja que se'n requereix mínim una l'any.	No hi ha cap gestió d'auditories de moment. Cal implementar-la.
15.3.2 Protecció d'eines d'auditoria	SI	Protegir eines d'auditoria d'accessos no permesos.	Algunes detectades per l'IDS. Accés restringit però cal impossibilitar la descàrrega.

A2. ANNEX II – ANÀLISI D'AMENACES

A continuació es presenta un llistat complet del càlcul de les amenaces pels diferents actius enumerats en la *Taula 6-2*, de l'apartat **6.5 - Anàlisi d'amenaces i impacte potencial**.

ACTIUS/AMENACES						
INSTAL·LACIONS	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[L.1],[L.2],[L.3],[L.4]		**0%**	**75%**	**75%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	50%	0%
[I] - DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,005	0%	0%	0%	50%	0%
[E] - ERRORS NO INTENCIONATS						
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	5%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	5%	0%	0%	0%
[A] - ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	5%	50%	50%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	75%	75%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	20%	20%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
[A.27] OCUPACIÓ ENEMIGA	0,002	0%	75%	0%	75%	0%
[L.5]		**0%**	**20%**	**20%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	50%	0%

[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	50%	0%
[E] – ERRORS NO INTENCIONATS						
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	5%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	5%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	5%	20%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	5%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	5%	5%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
[A.27] OCUPACIÓ ENEMIGA	0,002	0%	20%	0%	75%	0%
[L.6]		**0%**	**75%**	**75%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,016	0%	0%	0%	20%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	20%	0%
[E] – ERRORS NO INTENCIONATS						
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	5%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	5%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	5%	5%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	75%	75%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%

[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	5%	5%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
[A.27] OCUPACIÓ ENEMIGA	0,002	0%	75%	0%	75%	0%
DADES	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[D.1],[D.2],[D.3],[D.4],[D.5],[D.6],[D.7],[D.8]		**100%**	**100%**	**100%**	**100%**	**50%**
[E] - ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,016	0%	20%	75%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	75%	75%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,005	0%	0%	5%	0%	50%
[E.4] ERRORS DE CONFIGURACIÓ	0,016	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A] - ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	50%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	50%	50%	50%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,005	100%	100%	75%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	100%	75%	50%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	100%	100%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,005	0%	100%	0%	0%	0%
[D.11],[D.12]		**50%**	**75%**	**75%**	**100%**	**75%**
[E] - ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	75%	50%	75%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,002	0%	0%	5%	0%	75%
[E.4] ERRORS DE CONFIGURACIÓ	0,016	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%

[A] – ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	5%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	50%	20%	50%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	50%	75%	75%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	75%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	75%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	50%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	75%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
[D.9],[D.10],[D.13],[D.15]		**100%**	**100%**	**100%**	**100%**	**20%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	1	0%	20%	50%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,071	0%	50%	75%	20%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,016	0%	0%	5%	0%	20%
[E.4] ERRORS DE CONFIGURACIÓ	0,005	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	5%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	20%	20%	5%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	75%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	100%	50%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	50%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[D.16]		**50%**	**75%**	**75%**	**100%**	**20%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	20%	50%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,002	0%	0%	5%	0%	5%

[E.4] ERRORS DE CONFIGURACIÓ	0,016	0%	0%	5%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	5%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	20%	75%	75%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	50%	20%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	20%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,005	0%	50%	50%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
[D.17],[D.18],[D.19]		**20%**	**100%**	**75%**	**100%**	**75%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	20%	50%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,016	0%	0%	75%	0%	75%
[E.4] ERRORS DE CONFIGURACIÓ	0,005	0%	0%	50%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	100%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	5%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	5%	20%	75%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	20%	50%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	5%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	5%	0%	0%
[A.13] REPUDI	0,002	0%	0%	5%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%

[D.20]		**75%**	**100%**	**100%**	**100%**	**75%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	100%	100%	0%
[E.3] ERRORS DE MONITORITZACIÓ	0,071	0%	0%	50%	100%	75%
[E.4] ERRORS DE CONFIGURACIÓ	0,005	0%	0%	75%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.3] MANIPULACIÓ DE REGISTRES D'ACTIVITAT	0,002	0%	0%	20%	0%	0%
[A.4] MANIPULACIÓ DE LA CONFIGURACIÓ	0,002	75%	5%	50%	0%	0%
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	5%	100%	50%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	5%	20%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	20%	0%	0%
[A.13] REPUDI	0,002	0%	0%	5%	0%	5%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
CLAUS CRIPTOGRÀFIQUES	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[K.1]		**100%**	**100%**	**5%**	**75%**	**0%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,071	75%	20%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,002	0%	5%	5%	75%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	50%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,016	100%	100%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	100%	5%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	100%	5%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	50%	0%

[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[K.2]		**100%**	**100%**	**5%**	**100%**	**0%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,016	100%	100%	5%	20%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	5%	75%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	100%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	100%	5%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	5%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%		0%	0%	0%
[K.3]		**100%**	**75%**	**50%**	**100%**	**0%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	5%	100%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	100%	50%	0%	0%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	5%	5%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	50%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	50%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	50%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
SERVEIS	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[S.1], [S.2],[S.20],[S.21],[S.22],[S.31]		**75%**	**100%**	**100%**	**100%**	**20%**
[S.3],[S.4],[S.8],[S.9],[S.17],[S.23]		**75%**	**100%**	**100%**	**100%**	**20%**
[E] – ERRORS NO INTENCIONATS						

[E.1] ERRORS D'USUARI	0,016	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	75%	50%	100%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,005	0%	50%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	5%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	75%	100%	100%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	75%	100%	0%
[A.7] ÚS NO PREVIST	0,002	0%	75%	75%	20%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	50%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	50%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	75%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[S.5],[S.6],[S.7],[S.10],[S.11],[S.12],[S.13],[S.26]		**100%**	**100%**	**100%**	**100%**	**20%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,071	0%	5%	50%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	20%	75%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	5%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,016	0%	0%	0%		0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	100%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	75%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	50%		0%

[A.7] ÚS NO PREVIST	0,002	0%	75%	50%		0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	50%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	50%	0%	0%
[A.13] REPUDI	0,002	0%	0%	5%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[S.15]		**75%**	**100%**	**100%**	**100%**	**75%**
[E] - ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,016	0%	20%	75%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	50%	5%	75%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	20%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,071	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	50%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	75%	0%
[A] - ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	75%	100%	50%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	75%	50%	0%
[A.7] ÚS NO PREVIST	0,002	0%	50%	75%	50%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	20%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	50%	0%	0%
[A.13] REPUDI	0,002	0%	0%	20%	0%	75%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[S.18],[S.19],[S.24],[S.27]		**100%**	**100%**	**75%**	**100%**	**20%**
[S.16],[S.25],[S.28],[S.29]		**100%**	**100%**	**75%**	**100%**	**20%**
[E] - ERRORS NO INTENCIONATS						

[E.1] ERRORS D'USUARI	0,071	0%	100%	20%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	20%	75%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,016	0%	50%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,016	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	75%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	75%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	100%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	20%	5%	0%
[A.7] ÚS NO PREVIST	0,002	0%	5%	20%	5%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	50%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	50%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	75%	0%	0%
[A.13] REPUDI	0,002	0%	0%	5%	0%	20%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[S.30]		**50%**	**75%**	**75%**	**100%**	**5%**
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,071	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	5%	50%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,016	0%	20%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,016	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	50%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	75%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	50%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	50%	75%	5%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	50%	75%	0%

[A.7] ÚS NO PREVIST	0,002	0%	20%	5%	50%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	20%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	20%	0%	0%
[A.13] REPUDI	0,002	0%	0%	5%	0%	5%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	50%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
APLICACIONS/SOFTWARE	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[SW.1],[SW.2],[SW.3],[SW.4],[SW.5],[SW.6],[SW.7],[SW.8]		**100%**	**100%**	**100%**	**100%**	**50%**
[SW.9],[SW.10],[SW.11],[SW.12],[SW.13],[SW14],[SW.15],[SW.16]		**100%**	**100%**	**100%**	**100%**	**50%**
[SW.17]		**100%**	**100%**	**100%**	**100%**	**50%**
[I] – DESASTRES INDUSTRIALS						
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	75%	75%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	20%	100%	0%
[E.8] DIFUSIÓ DE MALWARE	1	0%	50%	50%	75%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,005	0%	20%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,071	0%	0%	75%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,071	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	100%	0%	0%	0%
[E.20] VULNERABILITATS DE PROGRAMA	0,005	0%	75%	50%	20%	0%
[E.21] ERRORS DE MANTENIMENT / ACTUALITZACIÓ SW	0,071	0%	0%	75%	50%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,005	100%	100%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	20%	50%	0%
[A.7] ÚS NO PREVIST	0,016	0%	20%	50%	20%	0%
[A.8] DIFUSIÓ DE MALWARE	0,002	0%	50%	50%	75%	0%

[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	50%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	75%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	50%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.22] MANIPULACIÓ DE PROGRAMES	0,002	0%	75%	75%	20%	0%
[SW.18],[SW.22],[SW.23],[SW.25],[SW.32],[SW.35], [SW.36],[SW.37]		**100%**	**100%**	**100%**	**100%**	**0%**
[SW.19],[SW.20],[SW.21],[SW.38]		**100%**	**100%**	**100%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,071	0%	20%	75%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	20%	75%	0%
[E.8] DIFUSIÓ DE MALWARE	0,002	0%	20%	20%	20%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	5%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	75%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	100%	0%	0%	0%
[E.20] VULNERABILITATS DE PROGRAMA	0,016	0%	20%	50%	75%	0%
[E.21] ERRORS DE MANTENIMENT / ACTUALITZACIÓ SW	0,071	0%	0%	50%	50%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,005	100%	100%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	75%	20%	50%	0%
[A.7] ÚS NO PREVIST	0,016	0%	20%	50%	50%	0%
[A.8] DIFUSIÓ DE MALWARE	0,002	0%	20%	20%	50%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	5%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%

[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%		0%	0%	0%
[A.22] MANIPULACIÓ DE PROGRAMES	0,002	0%	20%	75%	75%	0%
[SW.33],[SW.34]		**50%**	**75%**	**100%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	75%	100%	0%
[E.8] DIFUSIÓ DE MALWARE	0,002	0%	5%	20%	50%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	5%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
[E.20] VULNERABILITATS DE PROGRAMA	0,002	0%	5%	50%	75%	0%
[E.21] ERRORS DE MANTENIMENT / ACTUALITZACIÓ SW	0,002	0%	0%	5%	5%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	50%	50%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	20%	75%	0%
[A.7] ÚS NO PREVIST	0,002	0%	50%	20%	50%	0%
[A.8] DIFUSIÓ DE MALWARE	0,002	0%	5%	20%	5%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	5%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.22] MANIPULACIÓ DE PROGRAMES	0,002	0%	75%	75%	100%	0%
[SW.24],[SW.42]		**75%**	**100%**	**75%**	**100%**	**0%**
[SW.26],[SW.27],[SW28]		**75%**	**100%**	**75%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	100%	0%

[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,016	0%	20%	20%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,071	0%	20%	5%	50%	0%
[E.8] DIFUSIÓ DE MALWARE	0,002	0%	20%	20%	50%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	20%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,005	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	20%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[E.20] VULNERABILITATS DE PROGRAMA	0,016	0%	5%	20%	75%	0%
[E.21] ERRORS DE MANTENIMENT / ACTUALITZACIÓ SW	0,016	0%	0%	5%	50%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	75%	75%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,005	0%	100%	20%	20%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	50%	20%	0%
[A.8] DIFUSIÓ DE MALWARE	0,002	0%	5%	5%	5%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	20%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,005	0%	75%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.22] MANIPULACIÓ DE PROGRAMES	0,002	0%	50%	75%	75%	0%
[SW.30]		**50%**	**75%**	**100%**	**100%**	**0%**
[SW.29],[SW.31]		**50%**	**75%**	**100%**	**100%**	**0%**
[SW.39],[SW.40],[SW.41]		**50%**	**75%**	**100%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,071	0%	20%	5%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	20%	100%	0%

[E.8] DIFUSIÓ DE MALWARE	0,002	0%	20%	50%	50%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	75%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	20%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
[E.20] VULNERABILITATS DE PROGRAMA	0,002	0%	50%	20%	75%	0%
[E.21] ERRORS DE MANTENIMENT / ACTUALITZACIÓ SW	0,002	0%	0%	20%	100%	0%
[A] - ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,016	50%	75%	50%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,071	0%	50%	20%	5%	0%
[A.7] ÚS NO PREVIST	0,071	0%	20%	75%	50%	0%
[A.8] DIFUSIÓ DE MALWARE	0,016	0%	5%	5%	5%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	75%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	50%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,016	0%	50%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,005	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A.22] MANIPULACIÓ DE PROGRAMES	0,002	0%	5%	20%	75%	0%
MAQUINARI / HARDWARE	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[HW.1],[HW.2]		**0%**	**100%**	**100%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] - DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	50%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,002	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,071	0%	0%	0%	100%	0%

[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,002	0%	100%	100%	75%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	20%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	100%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	100%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	75%	75%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	75%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	100%	100%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	100%	0%	100%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[A.25] ROBATORI	0,002	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[HW.3]		**0%**	**100%**	**75%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	50%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,071	0%	0%	0%	50%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	20%	75%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,005	0%	0%	0%	50%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	75%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	100%	0%	100%	0%

[A] – ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	75%	50%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	20%	50%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	50%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	75%	0%	75%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[HW.5],[HW.6],[HW.7],[HW.8],[HW.9],[HW.11], [HW.12],[HW.24],[HW.30],[HW.31]		**0%**	**75%**	**50%**	**100%**	**0%**
[HW.4]		**0%**	**75%**	**50%**	**100%**	**0%**
[HW.10],[HW.27]		**0%**	**75%**	**50%**	**100%**	**0%**
[HW.13]		**0%**	**75%**	**50%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	75%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,005	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	5%	50%	75%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,016	0%	0%	0%	20%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,005	0%	0%	0%	100%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	50%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	20%	20%	75%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	20%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	50%	0%	0%

[A.23] MANIPULACIO D'EQUIPS	0,002	0%	50%	0%	100%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[A.25] ROBATORI	0,002	0%	75%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[HW.14],[HW.15],[HW.16],[HW.17],[HW.18], [HW.19],[HW.20]		**0%**	**75%**	**75%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	75%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,002	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	50%	20%	75%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	20%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	50%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	5%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	20%	20%	75%	0%
[A.7] ÚS NO PREVIST	0,002	0%	5%	5%	75%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	75%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	75%	0%	100%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[A.25] ROBATORI	0,002	0%	5%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[HW.21]		**0%**	**100%**	**50%**	**100%**	**0%**
[HW.22]		**0%**	**100%**	**50%**	**100%**	**0%**
[N] – DESASTRES NATURALS						

[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	50%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	50%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	75%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,002	0%	0%	0%	75%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	5%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	20%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	100%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	50%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	20%	20%	0%
[A.7] ÚS NO PREVIST	0,002	0%	20%	20%	5%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	50%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	75%	0%	20%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[HW.26]		**0%**	**75%**	**20%**	**100%**	**0%**
[HW.23]		**0%**	**75%**	**20%**	**100%**	**0%**
[HW.25],[HW.32]		**0%**	**75%**	**20%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	20%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	20%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	20%	0%

[I.2] DANYS PER AIGUA	0,016	0%	0%	0%	20%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,016	0%	0%	0%	20%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	50%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	50%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,005	0%	0%	0%	20%	0%
[E] - ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,002	0%	5%	5%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	50%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	20%	0%
[E.25] PÈRDUA D'EQUIPS	0,016	0%	75%	0%	100%	0%
[A] - ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	5%	5%	20%	0%
[A.7] ÚS NO PREVIST	0,002	0%	5%	5%	20%	0%
[A.11] ACCÈS NO AUTORITZAT	0,005	0%	50%	20%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	50%	0%	50%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,005	0%	75%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,005	0%	0%	0%	100%	0%
[HW.28],[HW.29]		**0%**	**5%**	**5%**	**100%**	**0%**
[N] - DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] - DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,005	0%	0%	0%	75%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,071	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,002	0%	0%	0%	50%	0%
[E] - ERRORS NO INTENCIONATS						

[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	5%	5%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,016	0%	0%	0%	75%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,016	0%	0%	0%	100%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	5%	0%	100%	0%
[A] - ATACS INTENCIONATS						
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,005	0%	5%	5%	20%	0%
[A.7] ÚS NO PREVIST	0,016	0%	5%	5%	20%	0%
[A.11] ACCÈS NO AUTORITZAT	0,005	0%	5%	5%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	5%	0%	20%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	5%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
COMUNICACIONS	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[COM.1],[COM.2],[COM.3]		**0%**	**100%**	**100%**	**100%**	**0%**
[COM.8],[COM.9],[COM.10]		**0%**	**100%**	**100%**	**100%**	**0%**
[COM.4],[COM.5]		**0%**	**100%**	**100%**	**100%**	**0%**
[I] - DESASTRES INDUSTRIALS						
[I.1] FALLADA SERVEI COMUNICACIONS	0,005	0%	0%	0%	100%	0%
[E] - ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	5%	20%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,005	0%	5%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	5%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	50%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	20%	0%
[E.19] FUGUES D'INFORMACIÓ	0,005	0%	75%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,005	0%	0%	0%	100%	0%
[A] - ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	0%	50%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	20%	5%	5%	0%
[A.7] ÚS NO PREVIST	0,002	0%	5%	5%	20%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	100%	0%	0%	0%

[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	100%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	75%	0%	0%
[A.12] ANÀLISI DE TRÀFIC	0,002	0%	50%	0%	0%	0%
[A.14] INTERCEPTACIÓ D'INFORMACIÓ (ESCOLTA)	0,002	0%	100%	0%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[COM.12]		**100%**	**100%**	**75%**	**100%**	**0%**
[COM.11]		**100%**	**100%**	**75%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						
[I.1] FALLADA SERVEI COMUNICACIONS	0,016	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,005	0%	20%	5%	50%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,016	0%	75%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%		0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%		0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%		0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%		0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	100%	75%	50%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	50%	50%	50%	0%
[A.7] ÚS NO PREVIST	0,016	0%	20%	20%	20%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	100%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	50%	50%	0%	0%
[A.12] ANÀLISI DE TRÀFIC	0,002	0%	75%	0%	0%	0%
[A.14] INTERCEPTACIÓ D'INFORMACIÓ (ESCOLTA)	0,002	0%	100%	0%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
[COM.7]		**50%**	**100%**	**20%**	**100%**	**0%**
[I] – DESASTRES INDUSTRIALS						

[I.1] FALLADA SERVEI COMUNICACIONS	0,071	0%	0%	0%	100%	0%
[E] – ERRORS NO INTENCIONATS						
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	20%	20%	20%	0%
[E.9] ERRORS DE REENCAMINAMENT	0,002	0%	100%	0%	0%	0%
[E.10] ERRORS DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,002	0%	0%	0%	0%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	0%	0%	0%	0%
[E.24] CAIGUDA SISTEMA PER ESGOTAMENT RECURSOS	0,002	0%	0%	0%	75%	0%
[A] – ATACS INTENCIONATS						
[A.5] SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI	0,002	50%	20%	20%	0%	0%
[A.6] ABÚS DE PRIVILEGIS D'ACCÈS	0,002	0%	20%	20%	50%	0%
[A.7] ÚS NO PREVIST	0,002	0%	0%	5%	50%	0%
[A.9] REENCAMINAMENT DE MISSATGES	0,002	0%	100%	0%	0%	0%
[A.10] ALTERACIÓ DE SEQÜÈNCIA	0,002	0%	0%	20%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	5%	0%	0%
[A.12] ANÀLISI DE TRÀFIC	0,002	0%	5%	0%	0%	0%
[A.14] INTERCEPTACIÓ D'INFORMACIÓ (ESCOLTA)	0,002	0%	5%	0%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	5%	0%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	50%	0%	0%	0%
[A.24] DENEGACIÓ SERVEI	0,002	0%	0%	0%	100%	0%
SUPORTS D'INFORMACIÓ	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[Media.1]		**0%**	**100%**	**100%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	75%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	100%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	100%	0%

[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,016	0%	0%	0%	50%	0%
[I.10] DEGRADACIÓ SUPORTS EMMAGATZEMAMENT	0,005	0%	0%	0%	75%	0%
[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,002	0%	5%	20%	5%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,016	0%	50%	75%	5%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	100%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,005	0%	0%	0%	5%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	100%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	5%	75%	50%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	5%	75%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	100%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	100%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	100%	0%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	50%	0%	20%	0%
[A.25] ROBATORI	0,002	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
[Media.2],[Media.3]		**0%**	**100%**	**100%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	100%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,016	0%	0%	0%	75%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,016	0%	0%	0%	50%	0%
[I.10] DEGRADACIÓ SUPORTS EMMAGATZEMAMENT	0,016	0%	0%	0%	100%	0%

[E] – ERRORS NO INTENCIONATS						
[E.1] ERRORS D'USUARI	0,016	0%	75%	20%	75%	0%
[E.2] ERRORS DE L'ADMINISTRADOR	0,002	0%	20%	50%	75%	0%
[E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ	0,016	0%	0%	100%	0%	0%
[E.18] DESTRUCCIÓ DE LA INFORMACIÓ	0,005	0%	0%	0%	50%	0%
[E.19] FUGUES D'INFORMACIÓ	0,002	0%	20%	0%	0%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	5%	0%
[E.25] PÈRDUA D'EQUIPS	0,016	0%	100%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,005	0%	50%	50%	50%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	75%	20%	0%	0%
[A.15] MODIFICACIÓ DELIBERADA D'INFORMACIÓ	0,002	0%	0%	75%	0%	0%
[A.18] DESTRUCCIÓ D'INFORMACIÓ	0,002	0%	0%	0%	75%	0%
[A.19] DIVULGACIÓ D'INFORMACIÓ	0,002	0%	75%	0%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	75%	0%	0%	0%
[A.25] ROBATORI	0,005	0%	100%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
EQUIPAMENTS AUXILIARS	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[AUX.1],[AUX.2],[AUX.3]		**0%**	**0%**	**50%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,016	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	100%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,005	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	75%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,005	0%	0%	0%	75%	0%
[I.9] INTERRUPCIO D'ALTRES SERVEIS I SUBMINISTRES	0,002	0%	0%	0%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,71	0%	0%	0%	5%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	0%	0%	100%	0%

[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	0%	50%		0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	0%	20%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	0%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[AUX.4],[AUX.5],[AUX.6]		**0%**	**0%**	**75%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	100%	0%
[N.2] DANYS PER AIGUA	0,005	0%	0%	0%	100%	0%
[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	100%	0%
[I.2] DANYS PER AIGUA	0,016	0%	0%	0%	100%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	100%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,005	0%	0%	0%	75%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,016	0%	0%	0%	75%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,005	0%	0%	0%	75%	0%
[I.9] INTERRUPCIO D'ALTRES SERVEIS I SUBMINISTRES	0,002	0%	0%	0%	50%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,71	0%	0%	0%	5%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%	0%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	0%	75%		0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	0%	20%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	0%	0%	50%	0%
[A.25] ROBATORI	0,002	0%	0%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	100%	0%
[AUX.7],[AUX.8],[AUX.9]		**0%**	**0%**	**0%**	**100%**	**0%**
[N] – DESASTRES NATURALS						
[N.1] FOC	0,002	0%	0%	0%	75%	0%
[N.2] DANYS PER AIGUA	0,002	0%	0%	0%	0%	0%

[I] – DESASTRES INDUSTRIALS						
[I.1] FOC	0,002	0%	0%	0%	75%	0%
[I.2] DANYS PER AIGUA	0,002	0%	0%	0%	0%	0%
[I.3] CONTAMINACIÓ MECÀNICA	0,002	0%	0%	0%	0%	0%
[I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA	0,002	0%	0%	0%	0%	0%
[I.6] TALL DE SUBMINISTRAMENT ELÈCTRIC	0,002	0%	0%	0%	0%	0%
[I.7] CONDICIONS INADEQUADES TEMPERATURA	0,002	0%	0%	0%	0%	0%
[I.9] INTERRUPCIO D'ALTRES SERVEIS I SUBMINISTRES	0,002	0%	0%	0%	0%	0%
[E.23] ERRORS DE MANTENIMENT / ACTUALITZACIÓ HW	0,002	0%	0%	0%	0%	0%
[E.25] PÈRDUA D'EQUIPS	0,002	0%		0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	0%	0%	0%	0%
[A.11] ACCÈS NO AUTORITZAT	0,002	0%	0%	0%	0%	0%
[A.23] MANIPULACIO D'EQUIPS	0,002	0%	0%	0%	0%	0%
[A.25] ROBATORI	0,002	0%	0%	0%	100%	0%
[A.26] ATAC DESTRUCTIU	0,002	0%	0%	0%	75%	0%
PERSONAL	**FREQ.**	**A**	**C**	**I**	**D**	**T**
[P.1]		**0%**	**100%**	**0%**	**100%**	**0%**
[E] – ERRORS NO INTENCIONATS						
[E.19] FUGUES D'INFORMACIÓ	0,016	0%	100%	0%	0%	0%
[E.28] INDISPONIBILITAT DEL PERSONAL	0,071	0%	0%	0%	100%	0%
[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	0%	0%	0%	0%
[A.28] INDISPONIBILITAT DEL PERSONAL	0,002	0%	0%	0%	100%	0%
[A.29] EXTORSIÓ	0,002	0%	75%	50%	20%	0%
[A.30] ENGINYERIA SOCIAL	0,005	0%	75%	50%	20%	0%
[P.2]		**0%**	**100%**	**0%**	**100%**	**0%**
[P.3]		**0%**	**100%**	**0%**	**100%**	**0%**
[E] – ERRORS NO INTENCIONATS						
[E.19] FUGUES D'INFORMACIÓ	0,016	0%	100%	0%	0%	0%
[E.28] INDISPONIBILITAT DEL PERSONAL	0,071	0%	0%	0%	100%	0%

[A] – ATACS INTENCIONATS						
[A.7] ÚS NO PREVIST	0,002	0%	0%	0%	0%	0%
[A.28] INDISPONIBILITAT DEL PERSONAL	0,002	0%	0%	0%	100%	0%
[A.29] EXTORSIÓ	0,002	0%	100%	50%	20%	0%
[A.30] ENGINYERIA SOCIAL	0,002	0%	100%	50%	50%	0%

A3. ANNEX III – DOCUMENTACIÓ AUDITORIA DE COMPLIMENT

A continuació es presenten certs documents per facilitar el seguiment de les no conformitats majors i menors trobades durant la realització de les auditories, així com també de les diferents observacions.

A3.1 MODEL DE FITXA PER NO CONFORMITATS MAJORS/MENORS

En la *Taula A3-1* es mostra un model de document per la realització del seguiment d'una no conformitat major o menor d'un control.

NO CONFORMITAT:	*codi*	**DATA:**	*DD/MM/AAAA*
TIPUS DE NO CONFORMTITAT:	□ MAJOR □ MENOR		
DESCRIPCIÓ DE LA NO CONFORMITAT:			
PARÀGRAF DE LA NORMA:		**DOCUMENT SGSI:**	
REPRESENTANT DE L'ORGANITZACIÓ:	**AUDITOR:**	**AUDITOR EN CAP:**	
SIGNATURA:	**SIGNATURA:**	**SIGNATURA:**	
ACCIÓ CORRECTORA PROPOSADA:			
		DATA D' IMPLANTACIÓ:	*DD/MM/AAAA*
		RESPONSABLE D'IMPLANTACIÓ:	
		RESPRESENTANT DE L'ORGANITZACIÓ:	
		SIGNATURA:	
REVISIÓ DE L'ACCIÓ CORRECTORA:			
RESULTAT:	□ SATISFACTORI □ NO SATISFACTORI □ APORTAR MÉS EVIDÈNCIES		
		DATA DE VERIFICACIÓ:	*DD/MM/AAAA*
		NOM DE L'AUDITOR:	
		SIGNATURA:	

DATA DE RESOLUCIÓ REQUERIDA:	*DD/MM/AAAA*		
TANCAMENT DE L'ACCIÓ CORRECTORA:			
RESULTAT:	□ SATISFACTORI □ NO SATISFACTORI		
		DATA DE TANCAMENT:	*DD/MM/AAAA*
		NOM DE L'AUDITOR:	
		SIGNATURA:	
RESOLUCIÓ DEL TANCAMENT:	□ SEGUIMENT EN PRÒXIMA AUDITORIA □ TANCAMENT DEFINITIU DE LA NC		

Taula A3-1: Fitxa per a seguiment de no conformitats majors i menors.

A3.2 MODEL DE FITXA PER OBSERVACIONS

La Taula A3-2 mostra un model de document per realitzar les anotacions de les diferents observacions realitzades per part de l'auditor.

NÚM. OBSERVACIÓ:	*codi*	**DATA:**	*DD/MM/AAAA*
DESCRIPCIÓ DE L'OBSERVACIÓ:			
PARÀGRAF DE LA NORMA:		**DOCUMENT DEL SGSI:**	
		NOM DE L'AUDITOR:	**NOM DE L'AUDITOR EN CAP:**
		SIGNATURA:	**SIGNATURA:**

Taula A3-2: Fitxa per a seguiment de les possibles observacions.

B. BIBLIOGRAFIA

[**CCN0**] El ENS y la normalización voluntaria relativa a SGSI's, *CCN-CERT*:

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=3053

[**DDA0**] La importància de la Declaració d'aplicabilitat per la norma ISO 27001, *Dejan Kosutic*

http://blog.iso27001standard.com/es/tag/declaracion-de-aplicabilidad/

[**INT0**] Políticas, normas, procedimientos de seguridad y otros documentos de un SGSI, *Javier Cao Avellaneda* en "*Blog de Seguridad de Inteco*"

http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Politicas_normas_procedimientos_de_seguridad_y_otros_documentos_de_un_SGSI

[**ISO0**] ISO 17799: Scope and implementation – Security Policy, Gregory *Yhan - MCAD.net*

http://www.17799.com/papers/iso17799scope.pdf

[**ISO1**] Código de buenas prácticas para la gestión de la seguridad de la información, *INDECOPI*

http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

[**ISO2**] ENS – ISO 27001, *http://www.esquemanacionaldeseguridad.info/*:

http://www.esquemanacionaldeseguridad.info/ens-iso-27001/

[**ISO3**] Resumen de controles ISO/IEC 27002:2005, www.iso27000.es:

http://www.iso27000.es/download/ControlesISO27002-2005.pdf

[**ISO4**] ISO 27001 Toolkit, *IsecT Ltd.*

http://www.iso27001security.com/html/iso27k_toolkit.html

[**ISO5**] How to achieve 27001 certification, *Sigurjon Thor Arnason i Keith D. Willett*

[**MAG0**] MAGERIT Libro I: Método, *Ministeri d'Hisenda i AAPP*

http://administracionelectronica.gob.es/recursos/pae_000021964.pdf

[**MAG1**] MAGERIT Libro II: Catálogo de elementos, *Ministeri d'Hisenda i AAPP*

http://administracionelectronica.gob.es/recursos/pae_000021965.pdf

[**MAG2**] MAGERIT Libro III: Guía de técnicas, *Ministeri d'Hisenda i AAPP*

http://administracionelectronica.gob.es/recursos/pae_000021966.pdf

[**PAE0**] Esquema Nacional de Seguridad, *Portal Administración Electrónica (PAE)*

http://www.administracionelectronica.gob.es/

[**PIL0**] Eina EAR/Pilar: http://www.pilar-tools.com/es/index.html

[**POL0**] Política de Seguridad del Ayuntamiento de Málaga, *Centro Municipal de Informática*

[**RFC0**] RFC 1244 – Site security handbook, *Internet Engineering Task Force (IETF)*

http://www.ietf.org/rfc/rfc1244.txt

[**UOC0**] Apunts de Sistemes de Gestió de la Seguretat de la Informació, *MISTIC 2012/2013*.