Implantació d'un SGSI en una administració local

Nom Estudiant: Verónica Alejaldre García

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

Nom Consultor: Arsenio Tortajada Gallego

Centre: UOC

Data Lliurament: 4 / 1 /2017

FITXA DEL TREBALL FINAL

Títol del treball:	Implantació d'un SGSI en una administració local
Nom de l'autor:	*Verónica Alejaldre García*
Nom del consultor:	Arsenio Tortajada Gallego
Data de lliurament (mm/aaaa):	*01/2017*
Àrea del Treball Final:	***Sistemes gestió seguretat informació***
Titulació:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resum del Treball (màxim 250 paraules):

Aquest Treball de Fi de Màster consisteix en la creació d'un Sistema de Gestió de Seguretat de la Informació (SGSI) que permeti a un organisme públic garantir el compliment de l'Esquema Nacional de Seguretat (ENS) a la vegada que incorpora les recomanacions recollides en la ISO/IEC 27002.

Abstract (in English, 250 words or less):

This Final Master is the creation of a Management System Information Security (ISMS) that allows a public organization to ensure compliance with the spanish National Security Scheme(ENS) while incorporating recommendations contained in the ISO / IEC 27002.

Paraules clau (entre 4 i 8):

ENS, ISO/IEC, 27007, SGSI

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

A continuació podem llegir un fragment de la informació continguda al web del Centro Criptológico Naciona (CCN):

“

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación ha vencido el 30 de enero de 2014.

El **Real Decreto 951/2015, de 23 de octubre**, de modificación del anterior RD establece que los sistemas deberán adecuarse a lo dispuesto **en un plazo de veinticuatro meses (4 de noviembre de 2017)**.

La adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de diversas cuestiones:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades. (Véase CCN-STIC 805 Política de seguridad de la información)
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.(Véase CCN-STIC 803 Valoración de sistemas en el Esquema Nacional de Seguridad)
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes. (Véase Magerit versión 3 y programas de apoyo –Pilar-)
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS. (Véase CCN-STIC 804 Medidas e implantación del Esquema Nacional de Seguridad)
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Véase CCN-STIC 806 Plan de adecuación del Esquema Nacional de Seguridad)
- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. (Véase serie CCN-STIC)
- Auditar la seguridad (Véase CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad y CCN-STIC 808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad)
- Informar sobre el estado de la seguridad (Véase CCN-STIC 815 Métricas e Indicadores en el Esquema Nacional de Seguridad y CCN-STIC 824 Informe del Estado de Seguridad)

“

Queda clar amb aquest fragment la necessitat d’implantar un SGSI en cada organisme públic, per tal de complir la legalitat vigent.

Amb aquest treball es pretén aconseguir uns coneixements bàsics i establir una base sobre la qual desenvolupar aquest SGSI real.

1.2 Objectius del Treball

El principal objectiu d’aquest TFM és establir una base per al compliment de l’ENS, així com implantar les bones pràctiques de la norma ISO/IEC 27002.

1.3 Enfocament i mètode seguit

El mètode de treball segui ha estat basat en les fases establertes gràcies a la guia que ofereix l'assignatura del TFM, i a les aportacions i suport del professor consultor.
Aquesta guia m'ha resultat excepcionalment útil i m'ha ajudat enormement a la realització d'aquest document.

1.4 Planificació del Treball

Gràcies a la mateixa guia de l'assignatura, el treball ha estat repartit en el temps de la següent manera:

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

Fase 2: Sistema de Gestió Documental

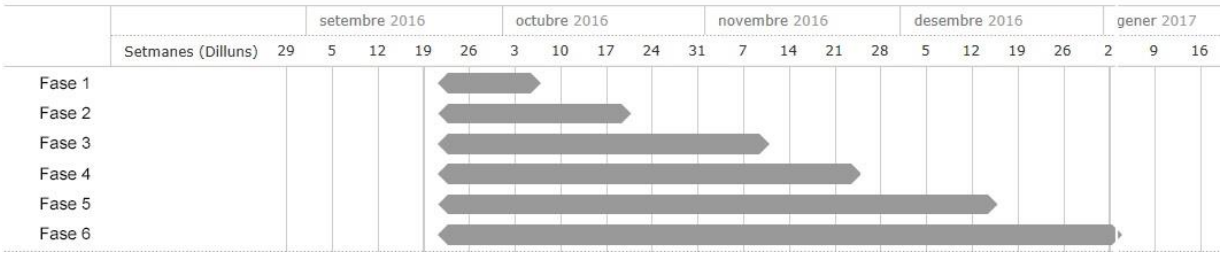
Fase 3: Anàlisis de riscos

Fase 4: Proposta de Projectes

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

Fase 6: Presentació de Resultats i entrega de Informes

En la imatge següent es pot veure la distribució d'aquestes fases en el temps:



Il·lustració 1: Temporalització del TFM

1.5 Sumari de productes obtinguts

Amb la realització d'aquest TFM s'han obtingut els següents productes o documents:

- Memòria final
- Resum executiu
- Presentació de defensa (ppt)
- Vídeo explicant el document de presentació

1.6 Breu descripció dels altres capítols de la memòria

La resta de capítols d'aquesta memòria corresponen al contingut desenvolupat a les diferents fases ja esmentades anteriorment, breument podem resumir aquests en:

Fase 1: Situació actual: Contextualització, objectius i anàlisis diferencial
Introducció al Projecte. Enfoc i selecció de l'empresa que serà objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisis diferencial de l'empresa amb respecte a la ISO/IEC 27001+ISO/IEC 27002

Fase 2: Sistema de Gestió Documental
Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI

Fase 3: Anàlisis de riscos
Elaboració d'una metodologia d'anàlisis de riscos: Identificació i valoració dels actius, amenaces, vulnerabilitats, càlcul del risc, nivell de risc acceptable i risc residual.

Fase 4: Proposta de Projectes
Avaluació de projectes que ha de portar a terme la Organització per alinear-se amb els objectius plantejats al Pla Director. Quantificació econòmica i temporal d'aquests.

Fase 5: Auditoria de Compliment de la ISO/IEC 27002:2013
Avaluació de controls, maduresa i nivell de compliment.

Fase 6: Presentació de Resultats i entrega de Informes
Consolidació dels resultats obtinguts durant el procés d'anàlisis. Realització dels informes i presentació executiva a Direcció. Entrega del projecte final.

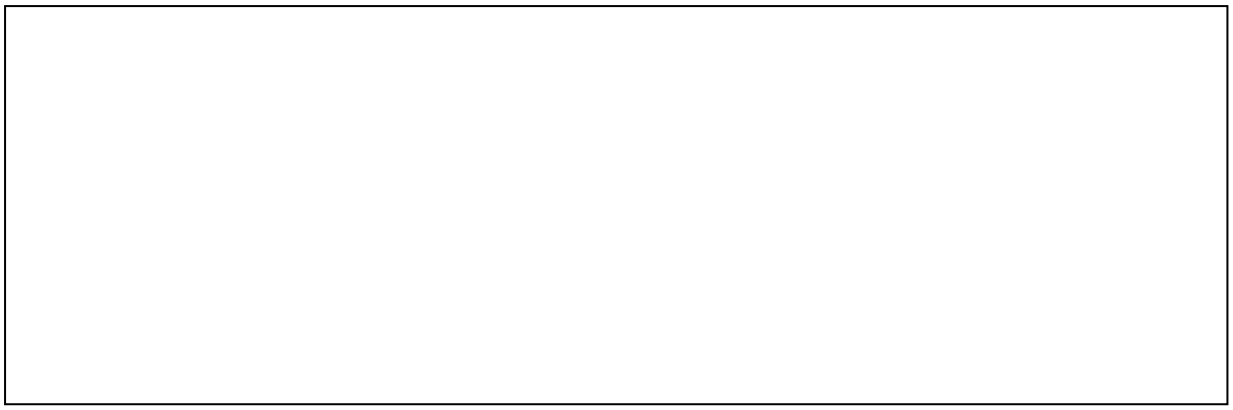
2. Contextualització: Descripció detallada de l'organització

Com a empresa objecte del projecte s'ha escollit una administració pública local, un Ajuntament en aquest cas, a continuació es detallen les dades rellevants:

Tipologia d'empresa: Ens públic local (Ajuntament)
Població del municipi: Menys de 5.000 habitants
Treballadors/res: Entre 60 i 75 treballadors/res
Treballadors/res amb accés a recursos informàtics: 60 treballadors/res
Centres de treball: 1 seu central, 4 seus remotes
Treballadors TIC: 1 coordinador, 1 HelpDesk

2.1. Organigrama de l'empresa

L'ens es troba dividit en àrees de treball dependents de les diferents regidories.
A continuació es pot veure l'esquema organitzatiu.
A l'annex 5 es mostra ampliat.



Il·lustració 2: Organigrama de l'entitat

2.1.1. Organització de seguretat

Pel que fa a l'organització de seguretat, no hi ha cap responsable ni àrea designat a realitzat la coordinació d'aquesta. Així, segons han anat sorgint les necessitats s'han anant establint algunes funcions de manera més o menys natural:

- **Accés físic:**

Pel que fa a l'accés físic, l'Enginyer Municipal s'encarrega de gestionar amb l'empresa de seguretat contractada per l'alarma els accessos dels usuaris habilitats amb clau de seguretat.

Es compta també amb un armari electrònic de claus pel qual s'ha d'habilitar usuaris i permís a les diferents claus, aquests es gestionen des de l'àrea TIC a petició del Departament de Personal.

Per últim, pel que fa a les claus físiques, es gestionen des del cos de Vigilants Municipals.

- **Accés lògic:**

Els accessos a equips informàtics, així com als diferents aplicatius de l'organització es gestionen des de l'Àrea TIC, a petició sempre del Departament de Personal.

2.1.2. Cultura

En general en l'organització la cultura en referència a la seguretat es nul·la:

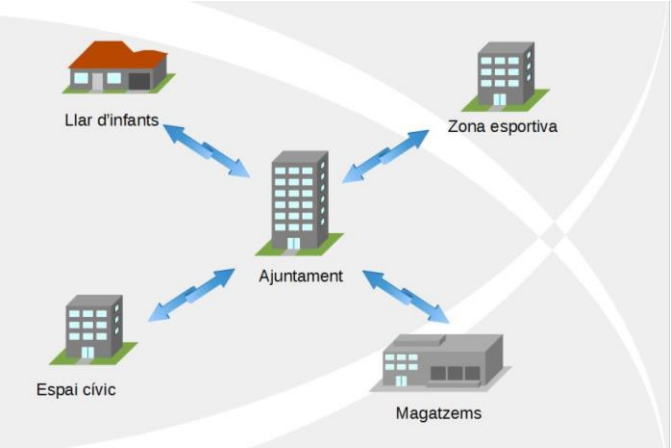
- Els usuaris no tenen cap consciència dels perills de seguretat, ni de les normes bàsiques de seguretat.
- No es duu a terme cap formació en seguretat.
- No hi ha cap responsable designat.

Cal destacar algunes excepcions en entre el personal en alguns punts, però, en general és des de l'Àrea TIC que es sol·liciten constantment autoritzacions al Departament de Personal per a peticions que el diferent personal realitza directament sense tenir en compte que s'han d'autoritzar de manera formal els accessos. Fins i tot, quan s'intenta explicar quin és el circuit adequat per les sol·licituds es donen situacions de rebuig

d'aquest personal envers a l'Àrea TIC, com si d'alguna manera no es volgués realitzar les gestions.

2.2. Instal·lacions

L'organització compta amb una seu central i diferents seus remotes.

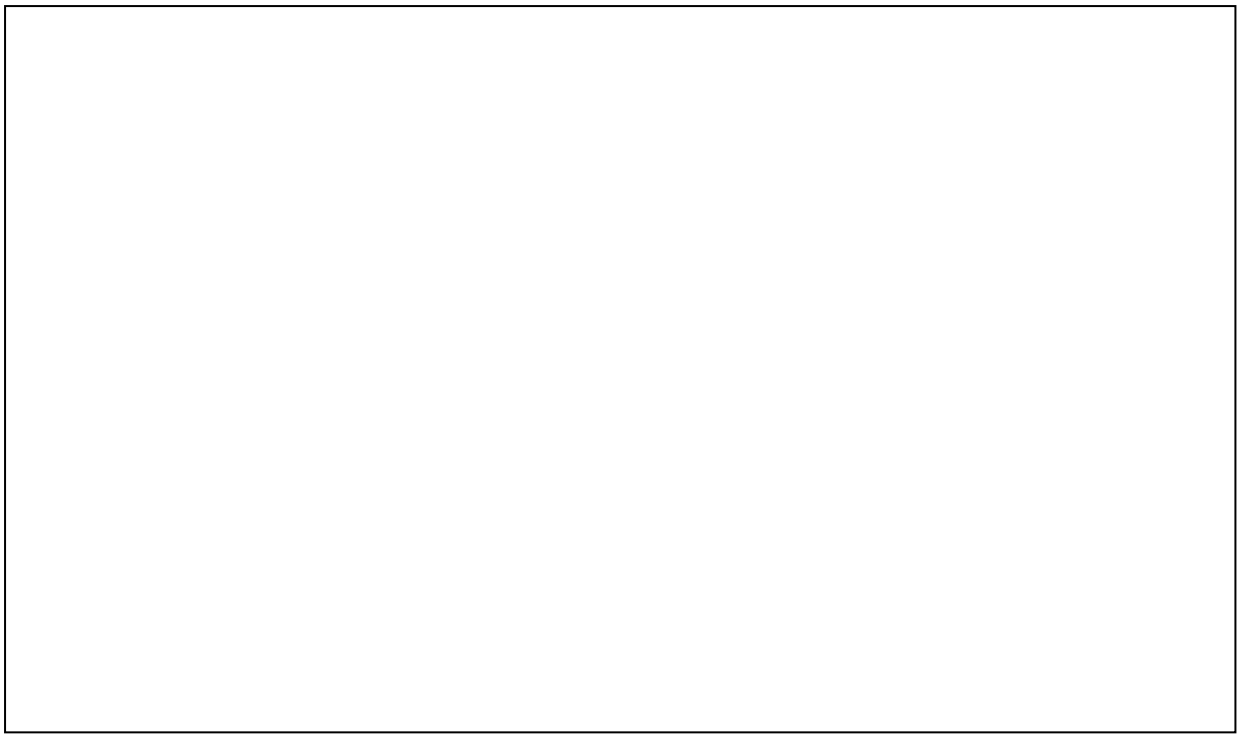


Il·lustració 3: Esquema de les seus

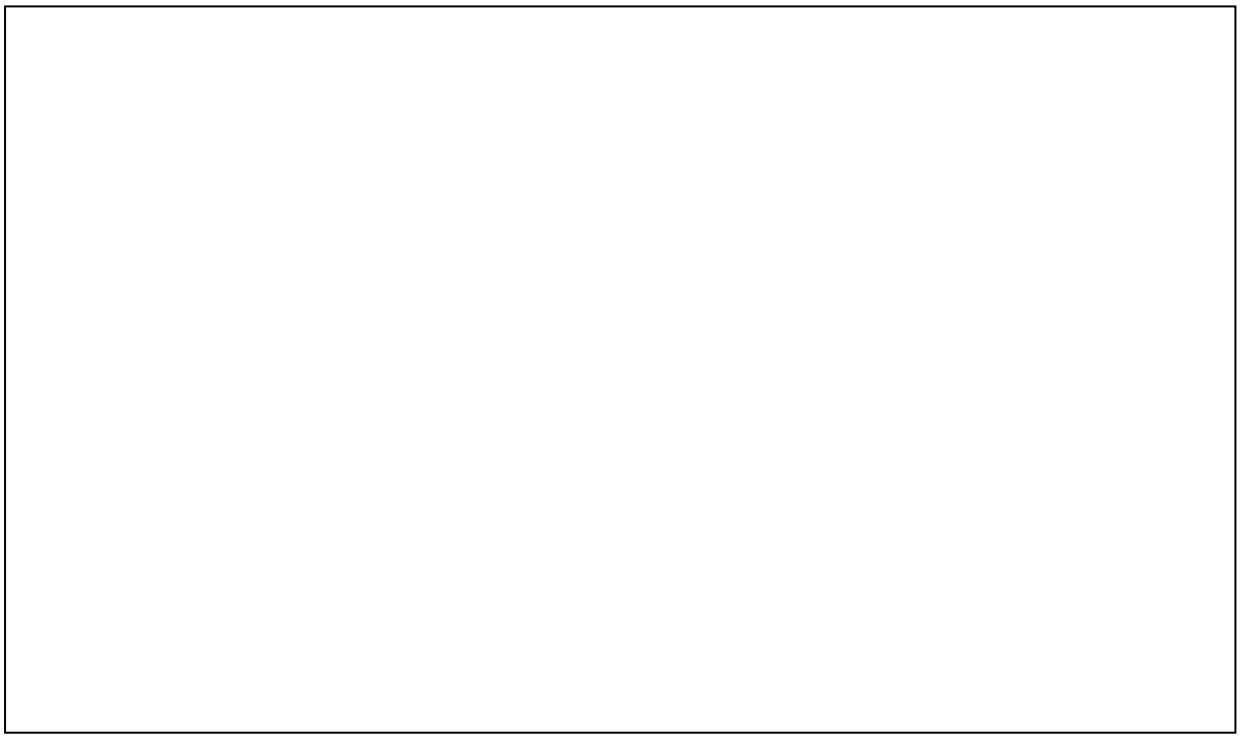
2.2.1. Plànols de la seu central

A continuació es mostren els plànols de la seu central, la qual consta de 3 plantes.

Il·lustració 4:Plànol de la planta 1 de la seu central



Il·lustració 5:Plànol de la planta 0 de la seu central



Il·lustració 6:Plànol de la planta -1 de la seu central

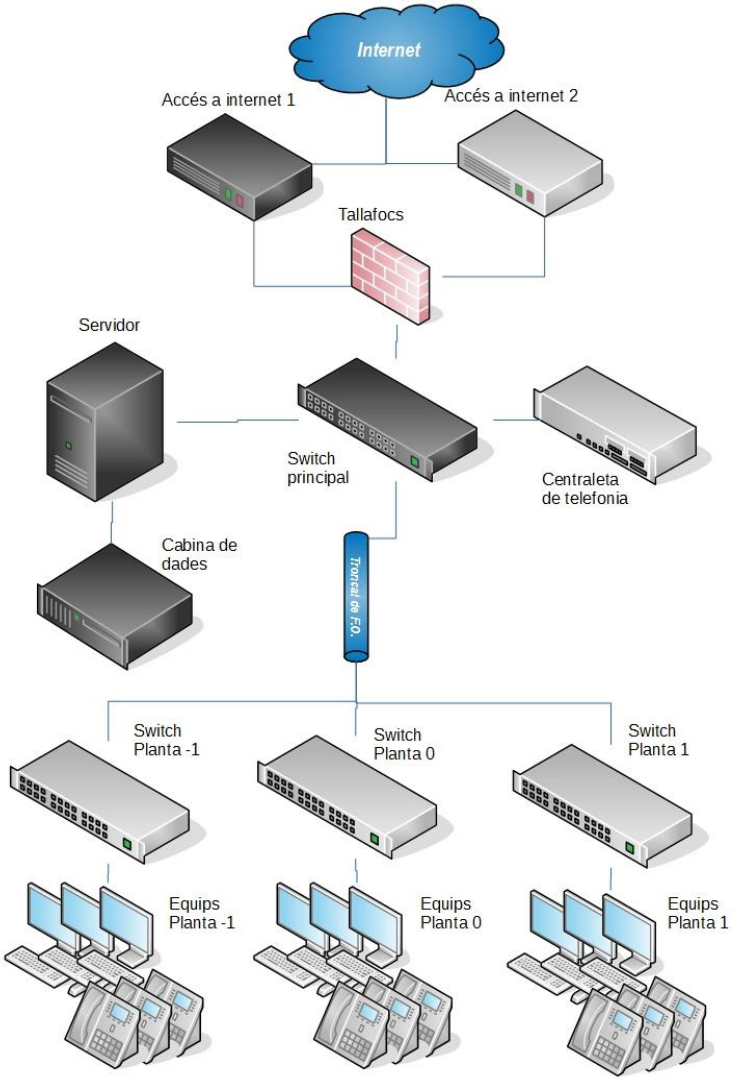
2.2.2. Estructura de la xarxa informàtica de la seu central

La xarxa informàtica de la seu centra està formada per:

- 2 connexions a internet
- 1 Tallafocs / router
- 1 switch central
- 1 servidor host amb sistema operatiu ESXi
- 1 Cabina de dades
- 1 Centraleta de telefonia IP
- 3 Switches que donen servei a cada planta de la seu central
- Les estacions de treball, telèfons IP i equips multifunció

Les estacions de treball compten amb un sistema d'alimentació ininterrompuda (SAI) individual, la resta d'equips de xarxa i servidors es connecten a un SAI central.

En la següent imatge es pot veure gràficament aquesta infraestructura.



Il·lustració 7:Esquema de la xarxa informàtica de la seu central

3. Objectius: Abast del pla director de Seguretat

La implantació d'aquest pla director de seguretat tindrà com a abast el compliment de l'Esquema Nacional de Seguretat pel que fa a les instal·lacions, personal i equipament de la seu central d'aquest ens.

4. Anàlisi de compliment inicial

Anàlisis diferencial de les mesures de seguretat i la normativa que tingui la Organització en relació a la Seguretat de la Informació.
En el cas que ens ocupa analitzarem els controls o mesures preventives, organitzats en 14 àrees i 35 objectius de control de la ISO/IEC 27002, i ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació i el compliment de l'Esquema Nacional de Seguretat (ENS):

4.1. Anàlisi de ISO/IEC 27002

A continuació es detallen els controls de seguretat amb el percentatge d'assoliment:

Efectivitat	
10%	**5. POLÍTICAS DE SEGURIDAD.**
10%	5.1 Directrices de la Dirección en seguridad de la información.
10%	5.1.1 Conjunto de políticas para la seguridad de la información.
10%	5.1.2 Revisión de las políticas para la seguridad de la información.
10%	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
10%	6.1 Organización interna.
10%	6.1.1 Asignación de responsabilidades para la segur. de la información.
10%	6.1.2 Segregación de tareas.
10%	6.1.3 Contacto con las autoridades.
10%	6.1.4 Contacto con grupos de interés especial.
10%	6.1.5 Seguridad de la información en la gestión de proyectos.
10%	6.2 Dispositivos para movilidad y teletrabajo.
10%	6.2.1 Política de uso de dispositivos para movilidad.
10%	6.2.2 Teletrabajo.
22,22%	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
50%	7.1 Antes de la contratación.
50%	7.1.1 Investigación de antecedentes.
50%	7.1.2 Términos y condiciones de contratación.
6,67%	7.2 Durante la contratación.
10%	7.2.1 Responsabilidades de gestión.
10%	7.2.2 Concienciación, educación y capacitación en segur. de la informac.
0%	7.2.3 Proceso disciplinario.
10%	7.3 Cese o cambio de puesto de trabajo.
10%	7.3.1 Cese o cambio de puesto de trabajo.

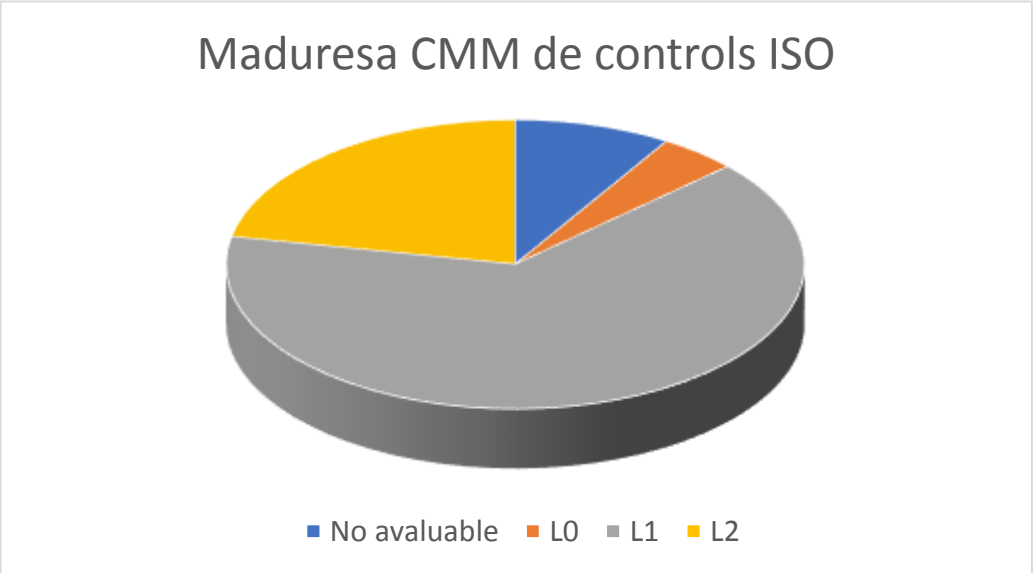
20%	**8. GESTIÓN DE ACTIVOS.**
10%	8.1 Responsabilidad sobre los Activos.
10%	8.1.1 Inventario de Activos.
10%	8.1.2 Propiedad de los Activos.
10%	8.1.3 Uso aceptable de los Activos.
10%	8.1.4 Devolución de Activos.
50%	8.2 Clasificación de la información.
50%	8.2.1 Directrices de clasificación.
50%	8.2.2 Etiquetado y manipulado de la información.
50%	8.2.3 Manipulación de Activos.
0%	8.3 Manejo de los soportes de almacenamiento.
0%	8.3.1 Gestión de soportes extraíbles.
0%	8.3.2 Eliminación de soportes.
0%	8.3.3 Soportes físicos en tránsito.
10%	**9. CONTROL DE ACCESOS.**
10%	9.1 Requisitos de negocio para el control de accesos.
10%	9.1.1 Política de control de accesos.
10%	9.1.2 Control de acceso a las redes y servicios asociados.
10%	9.2 Gestión de acceso de usuario.
10%	9.2.1 Gestión de altas/bajas en el registro de usuarios.
10%	9.2.2 Gestión de los derechos de acceso asignados a usuarios.
10%	9.2.3 Gestión de los derechos de acceso con privilegios especiales.
10%	9.2.4 Gestión de información confidencial de autenticación de usuarios.
10%	9.2.5 Revisión de los derechos de acceso de los usuarios.
10%	9.2.6 Retirada o adaptación de los derechos de acceso
10%	9.3 Responsabilidades del usuario.
10%	9.3.1 Uso de información confidencial para la autenticación.
10%	9.4 Control de acceso a sistemas y Aplicaciones.
10%	9.4.1 Restricción del acceso a la información.
10%	9.4.2 Procedimientos seguros de inicio de sesión.
10%	9.4.3 Gestión de contraseñas de usuario.
10%	9.4.4 Uso de herramientas de administración de sistemas.
10%	9.4.5 Control de acceso al código fuente de los programas.
10%	**10. CIFRADO.**
10%	10.1 Controles criptográficos.
10%	10.1.1 Política de uso de los controles criptográficos.
10%	10.1.2 Gestión de claves.
10%	**11. SEGURIDAD FÍSICA Y AMBIENTAL.**
10%	11.1 Áreas seguras.
10%	11.1.1 Perímetro de seguridad física.
10%	11.1.2 Controles físicos de entrada.
10%	11.1.3 Seguridad de oficinas, despachos y recursos.
10%	11.1.4 Protección contra las amenazas externas y ambientales.
10%	11.1.5 El trabajo en áreas seguras.

10%	11.1.6 Áreas de acceso público, carga y descarga.
10%	11.2 Seguridad de los equipos.
10%	11.2.1 Emplazamiento y protección de equipos.
10%	11.2.2 Instalaciones de suministro.
10%	11.2.3 Seguridad del cableado.
10%	11.2.4 Mantenimiento de los equipos.
10%	11.2.5 Salida de Activos fuera de las dependencias de la empresa.
10%	11.2.6 Seguridad de los equipos y Activos fuera de las instalaciones.
10%	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
10%	11.2.8 Equipo informático de usuario desatendido.
10%	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
44,29%	**12. SEGURIDAD EN LA OPERATIVA.**
10%	12.1 Responsabilidades y procedimientos de operación.
10%	12.1.1 Documentación de procedimientos de operación.
10%	12.1.2 Gestión de cambios.
10%	12.1.3 Gestión de capacidades.
10%	12.1.4 Separación de entornos de desarrollo, prueba y producción.
50%	12.2 Protección contra código malicioso.
50%	12.2.1 Controles contra el código malicioso.
50%	12.3 Copias de seguridad.
50%	12.3.1 Copias de seguridad de la información.
50%	12.4 Registro de actividad y supervisión.
50%	12.4.1 Registro y gestión de eventos de actividad.
50%	12.4.2 Protección de los registros de información.
50%	12.4.3 Registros de actividad del administrador y operador del sistema.
50%	12.4.4 Sincronización de relojes.
50%	12.5 Control del software en explotación.
50%	12.5.1 Instalación del software en sistemas en producción.
50%	12.6 Gestión de la vulnerabilidad técnica.
50%	12.6.1 Gestión de las vulnerabilidades técnicas.
50%	12.6.2 Restricciones en la instalación de software.
50%	12.7 Consideraciones de las auditorías de los sistemas de información.
50%	12.7.1 Controles de auditoría de los sistemas de información.
50%	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**
50%	13.1 Gestión de la seguridad en las redes.
50%	13.1.1 Controles de red.
50%	13.1.2 Mecanismos de seguridad asociados a servicios en red.
50%	13.1.3 Segregación de redes.
50%	13.2 Intercambio de información con partes externas.
50%	13.2.1 Políticas y procedimientos de intercambio de información.
50%	13.2.2 Acuerdos de intercambio.
50%	13.2.3 Mensajería electrónica.
50%	13.2.4 Acuerdos de confidencialidad y secreto.
50%	**14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓ**

50%	14.1 Requisitos de seguridad de los sistemas de información.
50%	14.1.1 Análisis y especificación de los requisitos de seguridad.
50%	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
50%	14.1.3 Protección de las transacciones por redes telemáticas.
-	14.2 Seguridad en los procesos de desarrollo y soporte.
-	14.2.1 Política de desarrollo seguro de software.
-	14.2.2 Procedimientos de control de cambios en los sistemas.
-	14.2.3 Revisión técnica de las Aplicaciones tras efectuar cambios en el sistema operativo.
-	14.2.4 Restricciones a los cambios en los paquetes de software.
-	14.2.5 Uso de principios de ingeniería en protección de sistemas.
-	14.2.6 Seguridad en entornos de desarrollo.
-	14.2.7 Externalización del desarrollo de software.
-	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
-	14.2.9 Pruebas de aceptación.
-	14.3 Datos de prueba.
-	14.3.1 Protección de los datos utilizados en pruebas.
10%	**15. RELACIONES CON SUMINISTRADORES.**
10%	15.1 Seguridad de la información en las relaciones con suministradores.
10%	15.1.1 Política de seguridad de la información para suministradores.
10%	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
10%	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
10%	15.2 Gestión de la prestación del servicio por suministradores.
10%	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
10%	15.2.2 Gestión de cambios en los servicios prestados por terceros.
10%	**16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓ.**
10%	16.1 Gestión de incidentes de seguridad de la información y mejoras.
10%	16.1.1 Responsabilidades y procedimientos.
10%	16.1.2 Notificación de los eventos de seguridad de la información.
10%	16.1.3 Notificación de puntos débiles de la seguridad.
10%	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
10%	16.1.5 Respuesta a los incidentes de seguridad.
10%	16.1.6 Aprendizaje de los incidentes de seguridad de la información.
10%	16.1.7 Recopilación de evidencias.
10%	**17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
10%	17.1 Continuidad de la seguridad de la información.
10%	17.1.1 Planificación de la continuidad de la seguridad de la información.
10%	17.1.2 Implantación de la continuidad de la seguridad de la información.
10%	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
10%	17.2 Redundancias.
10%	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
9%	**18. CUMPLIMIENTO.**
8%	18.1 Cumplimiento de los requisitos legales y contractuales.

0%	18.1.1 Identificación de la legislación aplicable.
10%	18.1.2 Derechos de propiedad intelectual (DPI).
10%	18.1.3 Protección de los registros de la organización.
10%	18.1.4 Protección de datos y privacidad de la información personal.
10%	18.1.5 Regulación de los controles criptográficos.
10%	18.2 Revisiones de la seguridad de la información.
10%	18.2.1 Revisión independiente de la seguridad de la información.
10%	18.2.2 Cumplimiento de las políticas y normas de seguridad.
10%	18.2.3 Comprobación del cumplimiento.

Com a resum d'aquesta taula, la següent imatge mostra gràficament els resultats:



Il·lustració 8: Maduresa CMM de controls ISO

4.2. Anàlisi de l'ENS

En tractar-se d'un organisme públic, s'ha de complir la normativa marcada per l'Esquema Nacional de Seguretat, a continuació es pot veure el resultat de l'anàlisi amb l'eina CLARA d'un dels equips de la xarxa corporativa:

Control ENS - Estat del control (% Compliment del control) *
OP.ACC.4 - Proceso de gestión de derechos de acceso (70%)
OP.ACC.5 - Mecanismos de autenticación (42,86%)
OP.ACC.6 - Acceso local (16,67%)
OP.EXP.2 - Configuración de seguridad (66,67%)
OP.EXP.5 - Gestión de cambios (100%)
OP.EXP.6 - Protección frente a código dañino (100%)
OP.EXP.8 - Registro de actividad de los usuarios (77,78%)
OP.EXP.10 - Protección de los registros de actividad (75%)
MP.EQ.2 - Bloqueo de puesto de trabajo (0%)
MP.EQ.3 - Protección de equips informàticos (100%)
MP.COM.3 - Protección de la autenticidad y de la integridad (50%)

5. Sistema de gestió documental

5.1. Política de Seguretat

Veure Annex 1: Política de Seguretat

5.2. Procediment d'Auditories Internes

Veure Annex 2: Auditories internes

5.3. Gestió d'Indicadors

L'ENS estableix una sèrie de mesures de protecció en el seu Annex II. En aquesta secció es planteja com mesurar dues facetes de la implantació d'aquestes mesures:

- Índex de maduresa. Per avaluar la implantació de les mesures en l'organització.
- Índex de compliment. Per avaluar la satisfacció de les mesures que s'exigeixen en funció dels nivells de seguretat o la categoria del sistema.

S'estableix un nivell de maduresa de referència per a cada mesura de protecció de l'Annex II de l'ENS. Se segueix una regla simple:

categoria del sistema	**nivell de maduresa de referència**
BAIXA	L2 - reproduïble però intuïtiu
MEDIA	L3 - procés definit
ALTA	L4 - gestionat i mesurable

5.4. Procediment de Revisió per Direcció

La Direcció de l'Organització, en aquest cas la Junta de Govern Local, ha de revisar anualment les qüestions més importants que han anat passant en relació al Sistema de Gestió de Seguretat de la Informació. Per aquesta revisió, la ISO/IEC 27001 defineix, tant els punts d'entrada, com els punts de sortida que han d'obtenir-se.

Així el procediment serà el següent:

Fase 1: Elaboració d'informe sobre estat de sistema:
El comitè de seguretat realitzarà (o delegarà), de forma anual, un informe d'estat.

Fase 2: Anàlisi de dades i avaluació de l'eficàcia del sistema
La Junta de Govern Local analitzarà les dades de l'informe presentat.

Fase 3: Informe de Revisió del Sistema
La Junta de Govern Local emetrà un informe de revisió del sistema.

5.5. Gestió de Rols i Responsabilitats

El sistema de Gestió de Seguretat de la Informació ha d'estar compost per un equip que s'encarregui de crear, mantenir, supervisar i millorar el Sistema.

A l'annex de política de seguretat es pot trobar la relació de rols i responsabilitats.

5.6. Metodologia d'Anàlisi de Riscos

S'estableix la sistemàtica que s'haurà de seguir per a calcular el risc i ha d'incloure bàsicament la identificació i valoració dels actius, amenaces i vulnerabilitats, en aquest cas s'**aplicarà la metodologia d'anàlisi MAGERIT.**

Veure Annex 3: MAGERIT

Nota: Al tractar-se d'una metodologia estandarditzada s'adjunta un document extern de presentació i explicació de la metodologia.

5.7. Declaració de Aplicabilitat

Aquest document que inclou tots els controls de Seguretat establerts a la Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada.

Veure Annex 4: Declaració d'aplicabilitat

6. Anàlisi de riscos

L'anàlisi de riscos permet determinar com és, quant val i com de protegit es troba el sistema. En coordinació amb els objectius, estratègia i política de l'Organització, les activitats de tractament dels riscos permeten elaborar un pla de seguretat que, implantat i operat, satisfaci els objectius proposats amb el nivell de risc que accepta la Direcció. Al conjunt d'aquestes activitats se li denomina Procés de Gestió de Riscos.

L'anàlisi de riscos proporciona un model del sistema en termes d'actius, amenaces i salvaguardes, i és la pedra angular per controlar totes les activitats amb fonament. La fase de tractament estructura les accions que s'emprenen en matèria de seguretat per satisfer les necessitats detectades per l'anàlisi.

6.1. Metodologia

Per tal de realitzar l'anàlisi de riscos de l'organització s'ha fet servir la metodologia d'anàlisi MAGERIT, metodologia d'anàlisi i gestió de riscos elaborada pel Consell Superior d'Administració Electrònica que estima que la gestió dels riscos és una pedra angular en les guies de bon govern.

Així l'anàlisi s'ha realitzat amb el suport de l'aplicatiu PILAR, eina del tipus EAR (Entorn d'Anàlisi de Riscos), les quals suporten l'anàlisi i la gestió de riscos d'un sistema d'informació seguint la metodologia Magerit i està desenvolupada i finançada parcialment pel CCN.

6.2. Actius

Actius essencials
- [per_RES] Registre d'entrades i sortides

actius
- [SW] Aplicacions
  - [SW.os_win_7] Windows 7
  - [SW.av_kav] Kaspersky
  - [SW.hypervisor_ESX01] ESX01
  - [SW.office_office365] Microsoft Office 365
  - [SW.os_Win2008] Windows server 2008 r2
  - [SW.os_Win2012] Windows server 2012
  - [SW.app_RegistreES] Servidor de Registre d'E/S
- [HW] Equips
  - [HW_pc.pc] Equips personals
- [HW.pc.a-ciutadana01] a-ciutadana01
- [HW.hosts] SERVERS
  - [HW.hosts.host_h01] Server01
- [HW.network] Elements de xarxa
  - [HW.network.switch_sw01] Switch 01
  - [COM] Comunicacions
  - [COM.ISDN_RDSI] RDSI Centraleta
  - [COM.ADSL_SC] ADSL Seu central
  - [COM.lan_LAN_SC] LAN Seu central
  - [COM.vpn_gimnas] VPN Gimnàs municipal
- [AUX] Elementos auxiliares
- [building_sc] Seu central
- [per] Personal
  - [ui] Usuaris interns
  - [op] Operador
  - [adm] Administrador de sistemes
  - [prov_Empresa1] Proveïdor 1

6.3. Descripció dels actius

[per_RES] Registre d'entrades i sortides

Domini de seguretat

[Dom_Critics] Elements crítics

Classes de Actius
- [essential] Actius essencials
  - [essential.info] informació
    - [D.per] dades de caràcter personal
      - [D.per.A] nivell: alto

[SW] Aplicacions
Domini de seguretat
[base] Elements base
Classes de Actius

[SW.os_win_7] Windows 7
Domini de seguretat
[base] Elements base
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.os] sistema operatiu
      - [SW.std.os.windows] windows

[SW.av_kav] Kaspersky
Domini de seguretat
[base] Elements base
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.av] anti virus

[SW.hypervisor_ESX01] ESX01
Domini de seguretat
[base] Elements base
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.hypervisor] hypervisor (gestor de la màquina virtual)

[SW.office_office365] Microsoft Office 365
Domini de seguretat
[base] Elements base
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.office] ofimàtica

[SW.os_Win2008] Windows server 2008 r2
Domini de seguretat
[Dom_Critics] Elements crítics
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.os] sistema operativo
      - [SW.std.os.windows] windows

[SW.os_Win2012] Windows server 2012
Domini de seguretat
[Dom_Critics] Elements crítics

Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.os] sistema operativo
      - [SW.std.os.windows] windows

[SW.app_RegistreES] Servidor de Registre d'E/S

Domini de seguretat
[base] Elements base
Classes de Actius
- [SW] Aplicacions (software)
  - [SW.std] estàndard (off the shelf)
    - [SW.std.app] servidor de Aplicacions

[HW] Equips

Domini de seguretat
[base] Elements base
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.pc] informàtica personal

[HW_pc.pc] Estacions de treball

Domini de seguretat
[base] Elements base
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.pc] informàtica personal

Dades
- nombre: 44

[HW.hosts] SERVERS

Domini de seguretat
[base] Elements base
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.host] grans equips (host)

[HW.hosts.host_h01] Server01

Domini de seguretat
[Dom_Critics] Elements crítics
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.host] grans equips (host)

[HW.network] Elements de xarxa

Domini de seguretat
[base] Elements base
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.network] suport de la xarxa

[HW.network.switch_sw01] Switch 01
Domini de seguretat
[base] Elements base
Classes de Actius
- [HW] Equipament informàtic (hardware)
  - [HW.network] suport de la xarxa
    - [HW.network.switch] commutador

[COM] Comunicacions
Domini de seguretat
[base] Elements base
Classes de Actius

[COM.ISDN_RDSI] RDSI Centraleta
Domini de seguretat
[base] Elements base
Classes de Actius
- [COM] Xarxes de comunicacions
  - [COM.ISDN] RDSI (xarxa digital)

[COM.ADSL_SC] ADSL Seu central
Domini de seguretat
[base] Elements base
Classes de Actius
- [COM] Xarxes de comunicacions
  - [COM.ADSL] ADSL

[COM.lan_LAN_SC] LAN Seu central
Domini de seguretat
[base] Elements base
Classes de Actius
- [COM] Xarxes de comunicacions
  - [COM.LAN] xarxa local

[COM.vpn_gimnas] VPN Gimnàs municipal
Domini de seguretat
[Dom_Critics] Elements crítics
Classes de Actius
- [COM] Xarxes de comunicacions
  - [COM.vpn] xarxa privada virtual

[AUX] Elementos auxiliares
Domini de seguretat
[base] Elements base
Classes de Actius

[prov_Empresa1] Proveïdor 1
Domini de seguretat
[base] Elements base

Classes de Actius
- [P] Personal
  - [P.prov] proveïdors

[building_sc] Seu central

Domini de seguretat
[base] Elements base
Classes de Actius
- [L] Instal·lacions
  - [L.building] edifici

Dades
- nombre: 1

[ui] Usuaris interns

Domini de seguretat
[base] Elements base
Classes de Actius
- [P] Personal
  - [P.ui] usuaris interns
  - [P.op] operadores
  - [P.adm] administradores de sistemes

Dades
- desc: usuaris bàsics
- nombre: 50

[op] Operador

Domini de seguretat
[base] Elements base
Classes de Actius
- [P] Personal
  - [P.op] operadores
  - [P.adm] administradores de sistemes

Dades
- nombre: 1

[adm] Administrador de sistemes

Domini de seguretat
[base] Elements base
Classes de Actius
- [P] Personal
  - [P.adm] administradores de sistemes

Dades
- nombre: 1

6.4. Valoració dels actius

La valoració dels actius es realitza segons:

- [D] disponibilitat
- [I] integritat de les dades
- [C] confidencialitat de les dades
- [A] autenticitat de los usuaris i de la informació
- [T] traçabilitat del servei i de les dades

Per realitzar aquesta valoració s'han establer els següents dominis de seguretat:

- [Dom_Critics] Elements crítics
- [base] Elements base

Així, la valoració dels actius seria:

Actiu	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[per_RES] Registre d'entrades i sortides	9	10	10	10	10
[SW.os_win_7] Windows 7	4	5	5	5	5
[SW.av_kav] Kaspersky	9	10	10	10	10
[SW.hypervisor_ESX01] ESX01	9	10	10	10	10
[SW.office_office365] Microsoft Office 365	4	5	5	5	5
[SW.os_Win2008] Windows server 2008 r2	9	10	10	10	10
[SW.os_Win2012] Windows server 2012	9	10	10	10	10
[SW.app_RegistreES] Servidor de Registre d'E/S	9	10	10	10	10
[HW.pcs] Estacions de treball	4	5	5	5	5
[HW.hosts.host_h01] Server01	9	10	10	10	10
[HW.network.switch_sw01] Switch 01	5	5	10	10	10
[COM.ISDN_RDSI] RDSI Centraleta	7	5	10	10	10
[COM.ADSL_SC] ADSL Seu central	7	5	10	10	10
[COM.lan_LAN_SC] LAN Seu central	7	5	10	10	10
[COM.vpn_gimnas] VPN Gimnàs municipal	7	5	10	10	10
[prov_Empresa1] Proveïdor 1	7	5	5	5	5
[building_sc] Seu central	7	5	10	10	10
[ui] Usuaris interns	4	5	5	5	5
[op] Operador	9	5	5	5	5
[adm] Administrador de sistemes	9	10	10	10	10

6.5. Anàlisis d'amenaces

L'anàlisi de les amenaces a les quals es veuen exposats els diferents actius es mostra a continuació, valorats segons els criteris de:

- [D] disponibilitat
- [I] integritat de les dades
- [C] confidencialitat de les dades
- [A] autenticitat de los usuaris i de la informació

Actius	**freqüència**	**[D]**	**[I]**	**[C]**	**[A]**
[B] Actius essencials					
[per_RES] Registre d'entrades i sortides					
[E] Equipament					
[SW] Aplicacions					
[SW.os_win_7] Windows 7	100	100	100	100	
[SW.av_kav] Kaspersky	100	100	100	100	
[SW.hypervisor_ESX01] ESX01	100	100	100	100	
[SW.office_office365] Microsoft Office 365	100	100	100	100	
[SW.os_Win2008] Windows server 2008 r2	100	100	100	100	
[SW.os_Win2012] Windows server 2012	100	100	100	100	
[SW.app_RegistreES] Servidor de Registre d'E/S	100	100	100	100	
[HW] Equips					
[HW_pc.pc] Estacions de treball	100	20	50		
[HW.hosts] SERVERS					
[HW.hosts.host_h01] Server01	100	20	100		
[HW.network] Elements de xarxa					
[HW.network.switch_sw01] Switch 01	100	20	50		
[COM] Comunicacions					
[COM.ISDN_RDSI] RDSI Centraleta	50	20	50	100	
[COM.ADSL_SC] ADSL Seu central	50	20	50	100	
[COM.lan_LAN_SC] LAN Seu central	50	20	50	100	
[COM.vpn_gimnas] VPN Gimnàs municipal	50	20	50	100	
[SS] Serveis subcontratats					
[prov_Empresa1] Proveïdor 1	10	50	50		
[L] Instal·lacions					
[building_sc] Seu central	100	10	50		
[P] Personal					
[ui] Usuaris interns	50	100	100		
[op] Operador	50	100	100		
[adm] Administrador de sistemes	50	100	100		

6.6. Impacte potencial

L'anàlisi de l'impacte potencial que pot suposar la materialització de les diferents amenaces, de nou, es valoren els següents paràmetres:

- [D] disponibilitat
- [I] integritat de les dades
- [C] confidencialitat de les dades
- [A] autenticitat de los usuaris i de la informació

Actiu	[D]	[I]	[C]	[A]
[B] Actius essencials				
[E] Equipament	9	10	10	10
[SW] Aplicacions				
[SW.os_win_7] Windows 7	4	5	5	5
[SW.av_kav] Kaspersky	9	10	10	10
[SW.hypervisor_ESX01] ESX01	9	10	10	10
[SW.office_office365] Microsoft Office 365	4	5	5	5
[SW.os_Win2008] Windows server 2008 r2	9	10	10	10
[SW.os_Win2012] Windows server 2012	9	10	10	10
[SW.app_RegistreES] Servidor de Registre d'E/S	9	10	10	10
[HW] Equips				
[HW_pc.pc] Estacions de treball	4	3	4	
[HW.hosts] SERVERS				
[HW.hosts.host_h01] Server01	9	8	10	
[HW.network] Elements de xarxa				
[HW.network.switch_sw01] Switch 01	5	3	9	
[COM] Comunicacions				
[COM.ISDN_RDSI] RDSI Centraleta	6	3	9	10
[COM.ADSL_SC] ADSL Seu central	6	3	9	10
[COM.lan_LAN_SC] LAN Seu central	6	3	9	10
[COM.vpn_gimnas] VPN Gimnàs municipal	8	3	9	10
[SS] Serveis subcontratats	4	4	4	
[prov_Empresa1] Proveïdor 1	4	4	4	
[L] Instal·lacions	7	2	9	
[building_sc] Seu central	7	2	9	
[P] Personal	8	10	10	
[ui] Usuaris interns	3	5	5	
[op] Operador	8	5	5	
[adm] Administrador de sistemes	8	10	10	

6.7. Resum de riscos

Amb les dades analitzades als punts anteriors podem classificar els riscos potencials de l'organització de la següent manera, per tal d'abordar posteriorment solucions:

- **Riscos físics**

  L'accés físic als diferents actius s'ha de controlar, gestionar, limitar i permetre fer un seguiment tant dels actius com dels accessos.

- **Riscos de programari**

  Tot el programari de l'organització està exposat a diferents riscos: virus, vulnerabilitats, etc. Caldrà també establir procediments per minimitzar aquests.

- **Riscos Humans**

  Els riscos humans als quals estan exposats els actius els podríem subclassificar en 3 tipologies:

  - **Involuntaris**

    Els involuntaris vindrien donats per possibles error del personal de l'organització, com per exemple esborrades accidentals de dades.

  - **Voluntaris**

    Els voluntaris, siguin per part de personal intern o de persones alienes a l'organització, però, en qualsevol cas serien accions totalment conscients.
    El resultat final i accions, podria ser similar a l'involuntari.

  - **Voluntaris amb tercers involuntari**

    Aquest cas el voldria separar per fer especial èmfasi en accions d'enginyeria social i similars.

- **Riscos naturals**

  Es tractaria de riscos associat a fets naturals, inundacions, focs naturals, etc.

7. Proposta de projectes

Amb la informació obtinguda en anterior punts d'aquest document cal establir unes línies de treball per abordar les diferents amenaces a les quals es veu sotmesa l'organització i mitigar així el risc actual.

Així, en base al resum de riscos exposat al punt 5.6., s'estableixen els següents projectes:

- Programa de millora del control d'accessos físics
- Millora del control d'accessos lògics
- Programa de formació i acompanyament en matèria de seguretat al personal de l'organització
- Programa de manteniment i actualització d'actius lògics i físics l'organització

7.1. Programa de millora del control d'accessos físics

Descripció:

Millorar el control d'accessos als diferents espais de l'organització, així com als actius que formen part de la mateixa. Suposaria una reducció dels riscos físics als quals està exposada l'Organització.
Així les accions previstes del projecte seran:

- Implantar càmeres de vídeovigilància en zones d'accés especialment sensible.
- Identificar al personal de l'organització amb targetes d'identificació i control d'accessos.
- Restringir tant al personal com a altres persones alienes a l'organització l'accés les diferents zones, segons l'autorització de la qual disposen.

Objectius:

- Realitzar un monitoratge dels accessos
- Adequar els accessos a les necessitats reals de les funcions que realitza el personal de l'organització
- Detectar i evitar accessos no autoritzats

Tots aquests objectius s'han de dur a terme tan a curt, mig com llar termini.

Pressupost:

- Càmeres: 4000 euros
- Aplicatiu de control d'accessos i presència (inclosa posada en marxa): 6000 euros
- Maquinari de control d'accessos i presència: 5000 euros
- Total inversió: 15000 euros
- Manteniment anual aplicatiu els següents anys: 4000 euros

Aquest pressupost no té em compte el temps dedicat pel personal intern de l'organització al projecte, el qual també s'hauria de quantificar.

Temporització:

La implantació del sistema es preveu en 3 mesos:

- Recerca de propostes i sol·licitar pressupostos: 1 mes
- Aprovació de la despesa: 2 setmanes
- Instal·lació i configuració inicial del maquinari i programari: 1 setmana
- Planificació del sistema i formació als departaments implicats en la gestió: 3 setmanes
- Formació a la resta del personal de l'organització: 2 setmanes

Punts de control:

Els punts del control els quals es faran servir per avaluar el procés de millora seran:

- Relació d'intents d'accés no autoritzat
- Relació d'accessos autoritzats
- Relació del personal autoritzat vinculat amb els recursos als quals té accés

7.2. Programa de millora del control d'accessos lògics

Descripció:

De la mateixa manera que cal realitzar una gestió dels accessos físics, també cal establir de manera controlada els accessos als recursos lògics o informàtics (bases de dades, aplicatius, documents), actius també objecte d'amenaces.
Així les accions previstes del projecte seran:

- Realitzar una avaluació de les funcions que realitza el personal de l'organització.
- Adequar els accessos lògics a aquestes funcions.
- Establir sistemes de control d'accessos no autoritzat.

Objectius:

- Realitzar un monitoratge dels accessos
- Adequar els accessos a les necessitats reals de les funcions que realitza el personal de l'organització
- Detectar i evitar accessos no autoritzats

Tots aquests objectius s'han de dur a terme tan a curt, mig com llar termini.

Pressupost:

- Renovació d'equips d'electrònica de xarxa (tallafocs): 10000 euros
- Renovació dels sistemes d'antivirus: 4000 euros
- Contractació d'un servei extern d'avaluació de vulnerabilitats i monitoratge d'accessos no autoritzats: 8000 euros
- Total inversió primer any: 22000 euros
- Manteniment anual els següents anys: 14000 euros (servei extern, antivirus, més renovació i/o incorporació de nous elements de seguretat de xarxa)

Aquest pressupost no té em compte el temps dedicat pel personal intern de l'organització al projecte, el qual també s'hauria de quantificar.

Temporització:

La implantació del sistema es preveu en 5 - 6 mesos:

- Recerca de propostes i sol·licitar pressupostos del servei extern: 1 mes
- Aprovació de la despesa: 2 setmanes
- Auditories inicials del servei extern: 2 setmanes
- Avaluació dels resultats i anàlisi de necessitats : 1 setmana
- Recerca de propostes i sol·licitar pressupostos de les necessitats de maquinari: 1 mes
- Aprovació de la despesa: 2 setmanes
- Instal·lació i configuració inicial del maquinari i programari: 1 setmana

Punts de control:

Els punts del control els quals es faran servir per avaluar el procés de millora seran:

- Relació d'intents d'accés no autoritzat
- Relació d'accessos autoritzats
- Relació del personal autoritzat vinculat amb els recursos als quals té accés

7.3. Programa de formació i acompanyament en matèria de seguretat al personal de l'organització

Descripció:

Resulta imprescindible comptar amb una plantilla conscienciada i formada en matèria de seguretat, tant física com lògica, així, caldrà realitzar una sèrie de formacions inicials a tot el personal, seguides per formacions que podríem dir de 'manteniment i actualització', així com donar tota aquesta formació al personal de nova incorporació, ja sigui temporal o fix.
Caldrà també disposar d'un 'paquet' més reduït potser per a personal puntual (proveïdors, etc..) que hagin d'accedir als recursos de l'organització.

Objectius:

- Dotar de formació al personal de l'organització com a persones alienes que accedeixin puntualment
- Disposar de material de formació i autoformació que abastin els diferents aspectes de seguretat
- Disposar de documents d'acceptació de normatives de seguretat que hagin de signar tant el personal de l'organització com persones alienes que accedeixin puntualment

Tots aquests objectius s'han de dur a terme tan a curt, mig com llar termini.

Pressupost:

El projecte es realitzarà amb recursos interns, per tant no preveure cap inversió, caldria quantificar el cost del temps invertit pel personal intern que es dedicarà al projecte.

Temporització:

La posada en marxa inicial del programa de formació es preveu en 5 - 6 mesos:
- Planificació de les accions formatives: 1 setmana
- Redacció dels materials de les accions formatives: 1 mes
- Redacció dels documents d'acceptació: 2 setmanes
- Realització d'accions formatives inicials: 2 mesos

Cal preveure posteriorment 1 jornada de formació per a cada persona de nova incorporació a l'empresa o 1 hora en el cas de personal extern puntual.

Pel que fa a les accions formatives de 'manteniment i actualització', es preveuen 2 jornades grupals a l'any, agrupades segons els diferents col·lectius.

Punts de control:

Els punts del control els quals es faran servir per avaluar el procés de millora seran:
- Relació de documents i material de formació
- Relació d'hores de formació impartides

7.4. Programa de manteniment i actualització d'actius lògics i físics de l'organització

Descripció:

Per tal de reduïr els riscos d'amenaces degudes a vulnerabilitats, virus, etc, cal mantenir tant el programari com el maquinari (firmware) actualitzat.
Així, cal establir un programa d'activitats de revisió i actualització d'aquests.

Objectius:

- Disminuir les vulnerabilitats de maquinari i programari

Aquest objectiu s'ha de dur a terme tan a curt, mig com llar termini.

Pressupost:

El projecte es realitzarà amb recursos interns, per tant no preveure cap inversió, caldria quantificar el cost del temps invertit pel personal intern que es dedicarà al projecte.

Temporització:

La posada en marxa inicial del programa de formació es preveu en 1,5 - 2 mesos:
- Inventari de maquinari i programari, amb la relació de fonts d'actualització: 1 setmana
- Planificació de les accions de manteniment: 1 setmana
- Realització d'accions manteniment inicials: 1 mes

Cal preveure posteriorment el temps que s'ha de dedicar a les accions de manteniment recurrent, segons s'hagi estipulat en la fase de planificació d'accions un cop avaluats els recursos.

Punts de control:

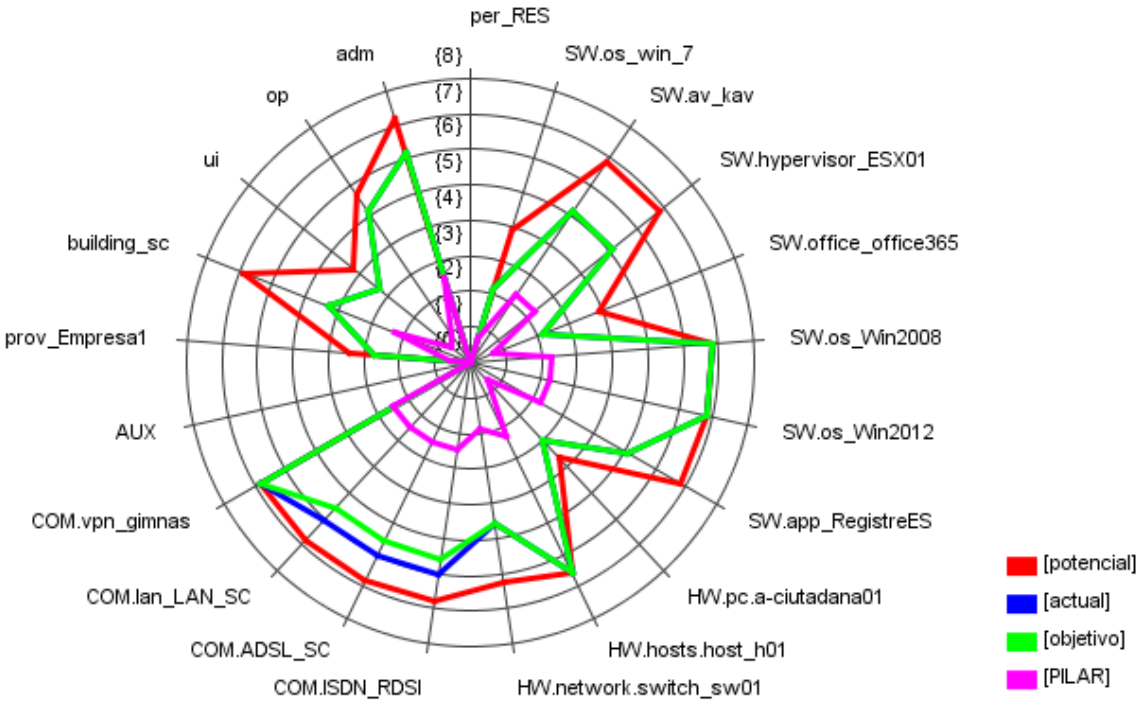
Els punts del control els quals es faran servir per avaluar el procés de millora seran:
- Relació d'actius de maquinari i programari.

- Relació d'accions de manteniment.

- Relació de vulnerabilitats resoltes en cada acció de manteniment.

7.5. Resultats del projectes

En el següent diagrama de radar podem veure els resultats tant del risc potencial, com de l'objectiu a assolir amb aquests projectes.



Il·lustració 9: Diagrama de risc

8. Conclusions

La realització d'aquest projecte estableix una base sobre la qual desenvolupar un SGSI real en una administració pública.
Crec que he assolit els objectius que havia marcat i sobretot la raó principal d'escollir no només aquest TFM sinó el Màster en si mateix, es evident que cal aprofundir en el detall dels actius, de la relació real amb el personal, així com dels riscos i amenaces, així com mantenir aquest com un procés viu que no ha de finalitzar, segons la metodologia de cicles P-D-C-A.
El procés de fases establert a l'assignatura m'ha ajudat molt, tot i que, en tractar-se d'un organisme públic he hagut d'adaptar els continguts, m'ha servir per documentar-me molt.
Com a conclusió final, puc dir que realitzar un SGSI real és una feina que portaria mesos de dedicació, fins i amb experiència prèvia en aquest àmbit (no era el cas), a partir d'aquest document tinc molta feina per endavant per poder aplicar-la amb meu lloc de treball.

9. Glossari d'acrònims

A continuació es detallen els acrònims utilitzats en aquest document:

SGSI: Sistemes de Gestió de la Seguretat de la Informació
TFM: Treball de Final de Màster
CPD: Centre de Processament de Dades
ISO: International Organization for Standardization
CMM: Model de Maduresa de la Capacitat

10. Bibliografia

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog.html#.WGvYslXhCUk

https://www.ccn-cert.cni.es/ens.html

Documentació de l'assignatura "Sistemes de Gestió de la Seguretat de la Informació", MISTIC, UOC

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

11. Annexos

ANNEX 1:
POLÍTICA DE SEGURETAT

ÍNDEX

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 1 de gener de de 2017.
Aquesta Política de Seguretat de la Informació és efectiva des d'aquesta data i fins que sigui reemplaçada per una nova Política.

2. INTRODUCCIÓ

L'organisme depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar a la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.
L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.
Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.
Els diferents departaments han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos a la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.
Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord a l'Article 7 del ENS.

2.1. PREVENCIÓ

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades pel ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.
Per garantir el compliment de la política, els departaments han de:

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

2.2. DETECCIÓ

Atès que els serveis es pot degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, els serveis han de monitorizar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons l'establert en l'Article 9 del ENS.

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

2.3. RESPOSTA

Els departaments han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

2.4. RECUPERACIÓ

Per garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

3. ABAST

Aquesta política s'aplica a tots els sistemes TIC i a tots els membres de l'organització, sense excepcions.

4. MISSIÓ

L'organisme té com a missió el servei a la ciutadania segons la normativa legal, la qual marca les seves funcions i responsabilitats.

5. MARC NORMATIU

Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics
Llei 39/2015, de 1'1 d'octubre del procediment administratiu comú de les administracions públiques
L'Esquema Nacional de Seguretat (ENS), regulat pel Real Decreto 3/2010 , de 8 de gener

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. COMITÈS: FUNCIONS I RESPONSABILITATS

El Comitè de Seguretat de la Informació no és un comitè tècnic, però ha de demanar regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions. El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els que hagi de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar de diferents formes i maneres:
• Grups de treball especialitzats interns, externs o mixtes.
• Assessoria externa.
• Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències.

El responsable de la seguretat de la informació del sistema (Responsable de la Seguretat en el ENS) és el/la secretari/ària del Comitè de Seguretat de la Informació i com tal:

- Convoca les reunions del Comitè de Seguretat de la Informació.
- Prepara els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elabora l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

El Comitè de Seguretat TIC reportarà a l'Àlcalde/ssa.
El Comitè de Seguretat TIC tindrà les següents funcions:

- Atendre les inquietuds dels responsables polítics i dels diferents departaments.
- Informar regularment l'estat de la seguretat de la informació als responsables polítics.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació.
- Elaborar l'estratègia d'evolució de l'Organització pel que fa a seguretat de la informació.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.
- Aprovar la normativa de seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Monitoritzar els principals riscos residuals assumits per l'Organització i recomanar possibles actuacions respecte d'ells.
- Monitoritzar l'acompliment dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Aprovar plans de millora de la seguretat de la informació de l'Organització. En particular vetllarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.
- Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
- Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes TIC des de la seva especificació inicial fins a la posada en operació. En particular haurà vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.

- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i / o entre diferents àrees de l'Organització, elevant aquells casos en els que no tingui prou autoritat per decidir.

El Comitè de Seguretat TIC estarà format pel/la Secretari/a-Interventor/, el/la Coordinador/a de l'àrea TIC, el/la Tècnic/a responsable del Departament de Personal.

6.2. ROLS: FUNCIONS, RESPONSABILITATS I DELEGACIONS

Degut a les característiques de l'organització els rols de:

- RESPONSABLE DE LA INFORMACIÓ
- RESPONSABLE DEL SERVEI
- RESPONSABLE DE LA SEGURETAT

Seran assignats a la mateixa persona, el/la Secretari/a – Interventor/a.

Pel que fa als rol de:

- RESPONSABLE DEL SISTEMA
- ADMINISTRADOR DE LA SEGURETAT DEL SISTEMA

Serà assignat al/la Coordinador/a de l'Àrea TIC

6.3. PROCEDIMENTS DE DESIGNACIÓ

El Responsable de Seguretat de la Informació serà nomenat per L'Alcalde/ssa a proposta del Comitè de Seguretat TIC. El nomenament es revisarà cada 2 anys o quan el lloc quedi vacant.
El Departament responsable d'un servei que es presti electrònicament d'acord a la Llei 11/2007 designarà al Responsable del Sistema, precisant les seves funcions i responsabilitats dins del marc establert per aquesta Política.

6.4. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Serà missió del Comitè de Seguretat TIC la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La Política serà aprovada per la Junta de Govern Local i difosa perquè la coneguin totes les parts afectades.

7. DADES DE CARÀCTER PERSONAL

L'organisme tracta dades de caràcter personal. El document de seguretat, al que tindran accés només les persones autoritzades, recull els fitxers afectats i els responsables corresponents. Tots els sistemes d'informació de l'organisme s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollits en l'esmentat Document de Seguretat.

8. GESTIÓ DE RISCOS

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

- regularment, almenys una vegada a l'any
- quan canviï la informació manejada
- quan canviïn els serveis prestats
- quan ocorri un incident greu de seguretat
- quan es reportin vulnerabilitats greus

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

9. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat de la Informació complementa les polítiques de seguretat de l'organisme en diferents matèries:

- Llistar referències a altres polítiques en matèria de seguretat.

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

V:\comunicació interna\Procediments\Política de seguretat.pdf

i impresa en l'arxiu municipal.

10. OBLIGACIONS DEL PERSONAL

Tots els membres de tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribi als afectats.
Tots els membres atendran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per atendre a tots els membres de , en particular als de nova incorporació.
Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura en què la necessitin per realitzar el seu treball. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

11. TERCERES PARTS

Quan presti serveis a altres organismes o manegi informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, se establiran canals para reporti i

coordinació dels respectius Comitès de Seguretat TIC i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que concerneixi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics de reporti i resolució d'incidències.
Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política.
Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

ANNEX 2:
AUDITORIES INTERNES

ÍNDEX

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 1 de gener de de 2017.
Aquest procediment és efectiu des d'aquesta data i fins que sigui reemplaçat nou document de procediment.

2. OBJECTE DE L'AUDITORIA

Donar compliment al que estableix l'article 34 i en l'Annex III del RD 3/2010, i per tant, verificar el compliment dels requisits establerts pel RD 3/2010 en els capítols II i III i en els annexos I i II.

Emetre una opinió independent i objectiva sobre aquest compliment de tal manera que permeti als responsables corresponents, prendre les mesures oportunes per a esmenar les deficiències identificades, si n'hi ha, i per satisfer internament, o bé enfront de tercers que puguin estar relacionats, sobre el nivell de seguretat implantat.

L'objectiu final de l'auditoria és sustentar la confiança que mereix el sistema auditat en matèria de seguretat; és a dir, calibrar la seva capacitat per garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat dels serveis prestats i la informació tractada, emmagatzemada o transmesa.

3. DESENVOLUPAMENT I EXECUCIÓ DE L'AUDITORIA

Com tota auditoria de sistemes de les tecnologies de la informació, que inclou normalment, els aspectes de seguretat dels sistemes, aquesta s'ha de fer d'una forma metodològica que permeti identificar clarament:

• L'Abast i Objectiu de l'Auditoria
• Els recursos necessaris i apropiats per realitzar l'auditoria (equip auditor)
• Les degudes comunicacions amb els responsables de l'organització que sol·licitin l'auditoria.
• La planificació preliminar o requisits d'informació previs al desenvolupament del programa d'auditoria, i a l'execució de les proves que es considerin necessàries.
• L'establiment d'un programa detallat d'auditoria amb les revisions i proves d'auditoria previstes.
• La presentació, dels resultats individuals de les proves, a les persones involucrades amb aquests resultats, per a la seva confirmació sense valoracions respecte als resultats finals.
• L'avaluació global dels resultats de l'auditoria en relació a l'objectiu i abast definits i als requisits del RD 3/2010.
• La confecció, presentació i emissió formal de l'Informe d'Auditoria.

La metodologia aplicada ha de permetre comprovar, a través dels registres i evidències d'auditoria, la consecució d'aquests passos, les limitacions que s'hagin pogut produir en el desenvolupament de les tasques, i les activitats realitzades.

Per a una consecució eficaç de l'auditoria, l'equip auditor verificarà que les mesures de seguretat per al sistema auditat s'ajusten als principis bàsics del RD 3/2010 (Article 4), i satisfan els requisits mínims de seguretat (article 11).

3.1. DEFINICIÓ DE L'ABAST I OBJECTIU DE L'AUDITORIA

L'abast i objectiu de l'auditoria han d'estar clarament definits, documentats i consensuats entre l'equip auditor i l'òrgan de les administracions públiques o entitats de dret públic vinculat o dependent (en endavant, òrgan de les administracions públiques) que hagi sol·licitat l'auditoria, i en sintonia amb l'article 34 del RD 3/2010.
Les auditories podran ser requerides pels responsables de cada organització amb competències sobre la seguretat del sistema d'informació objecte d'aquestes. Per tant, cal establir amb claredat abans de concretar la realització de l'auditoria, el objectiu i l'abast de la mateixa.
Considerant que les xarxes de comunicacions i sistemes de l'administració pública, tenen interconnexions amb entitats publiques i privades, la descripció detallada del abast de l'auditoria és essencial, és a dir, establir clarament el límit fins on es audita.
Les mesures de seguretat a auditar poden abastar mesures de naturalesa diversa (Organitzativa, física i lògica, entre d'altres), per tant, com a part de la definició del abast de l'auditoria, cal abans de començar-la, identificar els elements que entren dins d'aquest:

• Política de Seguretat.
• Valoració de la informació i els serveis, juntament amb la determinació de la categoria del sistema.
• Política de Signatura Electrònica i Certificats i serveis que utilitzen aquestes tècniques.
• Informació, serveis i altres recursos subjectes a l'auditoria.
• Tipus de dades que es manegen així com la normativa que els sigui aplicable.
Per exemple, dades de caràcter personal.
• Òrgan de les AAPP responsable i personal afectat per l'auditoria.
• Connexions externes amb altres organismes públics o privats.
• És imprescindible que es defineixi, preliminarment, si hi ha alguna informació que, per indicació del Responsable del Sistema, del Servei o del de Seguretat, no estarà accessible als auditors, i ni tan sols al cap de l'equip d'auditoria, el qual ha d'avaluar si aquesta és una limitació per realitzar l'auditoria.
• Legislació que afecta el sistema d'informació auditat: si bé aquesta auditoria és requerida per a les mesures de seguretat establertes pel RD 3/2010, aquesta norma també esmenta les dades de caràcter personal i per tant cal considerar la legislació aplicable a aquest tipus de dades.
• Una altra legislació que pugui ser aplicable, d'acord amb el que estableix la Llei 6/1997, de 14 d'abril, d'organització i funcionament de la Administració General de l'Estat i Llei 50/1997, de 27 de novembre, del Govern; els estatuts d'autonomia, lleis autonòmiques i normes de desenvolupament; i la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim Local, respectivament.

Per assegurar la independència objectiva de l'equip auditor, les tasques d'auditoria no s'inclouran en cap cas l'execució d'accions que puguin ser considerades com responsabilitats de consultoria o similars (implantació o modificació de programari relacionat amb el sistema auditat, redacció de documents requerits pel RD 3/2010 o procediments d'actuació, com tampoc possibles recomanacions de productes concrets de programari, entre d'altres).

3.2. EQUIP AUDITOR

L'equip auditor ha d'estar compost per un equip de professionals (Cap de l'equip d'auditoria, auditors, i experts) que garanteixi que es disposa dels coneixements (de acord a l'abast establit per a l'auditoria) suficients per assegurar l'adequada i ajustada realització de l'auditoria.
Aquest equip podrà estar format per auditors interns i / o externs o un combinació de tots dos, però en tot cas, cal complir amb els següents requisits:
• Si l'equip d'auditoria és intern, aquest ha de ser totalment independent de l'organització, sistemes o serveis que siguin o puguin ser objecte de l'auditoria. Per tant, l'equip d'auditoria hauria de pertànyer al grup d'Auditoria / Control Intern / Intervenció, o a un grup amb responsabilitats similars constituït com a tal, que asseguri la seva independència i objectivitat.
• Si participen auditors interns i externs, s'ha d'establir quin equip és responsable de la supervisió i realització de l'auditoria, i de l'emissió del informe, i conseqüentment, dels resultats de l'auditoria. El programa d'auditoria ha d'establir amb claredat la responsabilitat i assignació de funcions a cada integrant de l'equip auditor.
• Siguin auditors externs o interns, o un equip mixt, la propietat dels documents de treball i de les evidències, així com la responsabilitat per la emissió de l'informe i el seu contingut han de ser sempre inequívoques tant en la obertura de l'auditoria, com en el seu informe final.
• Si la realització de l'auditoria ha estat encarregada a un equip extern (Organització privada o pública), els integrants hauran de signar les preceptives clàusules de confidencialitat, incloent les clàusules aplicables de la legislació de protecció de dades de caràcter personal. A l'Annex D d'aquesta guia es inclou un model aplicable.
• Si l'auditoria és liderada per un equip d'Auditoria Interna, però amb la incorporació d'experts independents, aquests també han de signar una clàusula de confidencialitat.

L'equip auditor, en el disseny de les seves proves i revisions, no s'ha de limitar a la revisió de documents, ja que l'objectiu de l'auditoria és obtenir evidències eficaces per avaluar i sustentar si, a la pràctica, les mesures de seguretat auditades són adequades per protegir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació tractada, emmagatzemada o transmesa pel sistema auditat

Els components de l'equip d'auditoria hauran de tenir una formació suficient en auditoria de sistemes d'informació, i en seguretat. Si es considera necessari per la complexitat tecnològica o dimensions de l'entorn a auditar, es podran incorporar experts en determinades matèries.

El cap de l'equip auditor ha d'assegurar que:
• Disposa dels coneixements tècnics necessaris per a abordar l'auditoria d'una forma eficient.
• Es realitzen les accions necessàries, en l'etapa preliminar, per garantir que tots els integrants de l'equip entenen i coneixen l'estructura organitzativa i tècnica del sistema a auditar, els serveis que presta, i l'objectiu i l'abast de l'auditoria.
• Tots els auditors coneixen el RD 3/2010, i, en la mesura de les tasques assignades, els requisits de seguretat d'una altra legislació aplicable, i en particular, la relativa a la protecció de dades de caràcter personal.

Per a la realització de l'auditoria cal fer una planificació preliminar que, fonamentalment, consisteix a establir els requisits d'informació i documentació necessaris i imprescindibles per a:
• Establir i desenvolupar el programa d'auditoria.
• Concretar els coneixements necessaris de l'equip d'auditoria.
• Definir l'agenda de revisions, reunions i entrevistes.

• Definir les revisions i proves a realitzar.
• Adjudicar les tasques als components de l'equip d'auditors i experts.
• Si es realitza una auditoria conjunta amb la requerida pel RD 1720/2007, en les seves articles 96 i 110, identificar quines mesures de seguretat entren en l'abast de aquesta última. L'objectiu d'eficiència és que la revisió d'una mateixa mesura sigui auditada una sola vegada, tenint en compte els objectius relacionats amb el RD 3/2010, i amb els del RD 1720/2007.

La documentació mínima a requerir per concretar la planificació en detall de la auditoria del compliment del RD 3/2010, és:
• Documents signats per l'òrgan superior corresponent, segons s'estableix al RD 3/2010, que mostrin el coneixement i l'aprovació formal de les decisions en matèria de política de seguretat.
• Organigrama dels serveis o àrees afectades, amb descripció de funcions i responsabilitats.
• Identificació dels responsables: de la informació, dels serveis, de la seguretat i del sistema, segons es contemplen en el RD 3/2010.
• Descripció detallada del sistema d'informació a auditar (programari, maquinari, comunicacions, equipament auxiliar, ubicacions i similars).
• Identificació de la categoria del sistema segons l'Annex I del RD 3/2010.
• Nivells de seguretat definits.
• La Política de Seguretat.
• La Política de Signatura Electrònica i Certificats (si es fan servir aquestes tecnologies).
• La normativa de seguretat.
• Descripció detallada del sistema de gestió de la seguretat i la documentació que ho substància.
• Informes d'anàlisi de riscos.
• La Declaració de Aplicabilitat.
• Decisions adoptades per gestionar els riscos.
• Relació de les mesures de seguretat implantades.
• Relació de registres d'activitat pel que fa a les mesures de seguretat implantades.
• Informes d'altres auditories prèvies de seguretat relacionats amb els sistemes i serveis inclosos en l'abast de l'auditoria, com podria ser, l'informe de la auditoria biennal de protecció de dades de caràcter personal, o d'auditories prèvies amb el mateix objectiu i abast que l'auditoria a començar.
• Informes de seguiment de deficiències detectades en auditories prèvies de seguretat, i relacionades amb el sistema a auditar.
• Llista de proveïdors externs els serveis es veuen afectats o entren dins el abast de l'auditoria, i evidències del control realitzat sobre aquests serveis.

Segons la disponibilitat d'aquesta documentació, i d'acord amb els responsables de la informació, del servei i del responsable de seguretat, el cap de l'equip d'auditoria determinarà si és necessari rebre una còpia, o bé, segons el cas, n'hi ha prou amb una presentació d'aquesta documentació, per part d'aquests responsables.

No obstant això, és aconsellable per a una planificació ajustada de les proves en detall, que es pugui disposar de còpies (en suport paper o electrònic) d'alguna d'elles com evidència, o per facilitar la planificació de les proves i assignació de tasques als integrants de l'equip auditor. En tots els casos l'equip auditor mantindrà una llista actualitzada de la documentació sol·licitada i la seva situació pel que fa a si va ser rebuda còpia, o es va permetre l'accés per a la seva revisió.

3.4. PROGRAMA D'AUDITORIA

Cada entorn a auditar serà diferent i amb les seves pròpies configuracions i estructura organitzativa, per tant, cal tenir-les en compte a l'hora de:
a) dissenyar les revisions i proves d'auditoria,
b) definir en què consistirà cadascuna d'elles
c) establir els recursos necessaris (l'equip d'auditoria i dels serveis auditats).

Per a la planificació de l'auditoria s'han de tenir en compte les següents premisses:
• Els criteris organitzatius de l'òrgan responsable del sistema auditat i la descripció de les funcions del personal afectats per aquest sistema.
• Els elements de la seguretat que poden auditar mitjançant la revisió documentació, observació, i / o entrevistes.
En el cas concret de realitzar simultàniament l'auditoria requerida pel RD 1720/2007, cal identificar la documentació específica per a aquesta auditoria, addicionalment a la necessària per a l'auditoria del RD 3/2010, com per exemple, el Document de Seguretat aplicable.
• La selecció de mesures de seguretat a verificar que fa al seu compliment tal i com han estat aprovades.
• Les revisions que haurien de fer mitjançant l'execució de proves tècniques (Accessos, visualització de registres, edició de paràmetres de seguretat, observació i fotografia, si és aplicable, de les mesures de seguretat física, etc.), establint mostres d'elements a revisar. L'objectiu, en aquest cas, és comprovar el compliment i l'observança de determinades normes de seguretat.

Atès que el RD 1720/2007 requereix, en ocasions, determinades mesures de seguretat, que és possible que no es contemplin en les mesures de seguretat adoptades, com a resultat de l'anàlisi de riscos segons els requisits del RD 3/2010, aquestes mesures han de ser identificades per verificar el seu compliment, com ara la verificació mensual dels registres d'accés.
• Les proves podran realitzar-se en base a mostres, però l'equip auditor ha sustentar que la mostra d'elements seleccionada per a una prova determinada, és prou representativa, per garantir la solvència dels resultats.
• Les evidències que s'espera obtenir en cada prova i quines són ineludibles per documentar la realització de la prova.
• Assignació de tasques a cada integrant de l'equip d'auditoria segons la seva qualificació i experiència, i assignació de tasques als experts. Caldrà deixar constància de la supervisió del seu treball.
• Si hi ha informes recents d'auditoria prèvies (internes o externes) que hagin inclòs la revisió d'elements afectats per la present auditoria, aquests podran considerar en la planificació i no repetir proves, sempre que:

  • D'acord a la informació inicial rebuda, no s'hagin modificat les mesures de seguretat, i es pugui tenir accés a les evidències de les proves realitzades en el seu moment. Si les mesures s'han modificat, per qualsevol circumstància, ja sigui per raons de millora contínua, o per solucionar deficiències identificades en l'auditoria anterior, la mesura de seguretat es tornarà a revisar.
  • Aquestes auditories prèvies hagin tingut el grau d'independència objectiva i qualificació, similar al requerit per a la realització de l'auditoria del RD 3/2010.

Els elements a incloure en la planificació de l'auditoria, com a elements mínims a considerar són els següents, tenint com a referència així mateix l'Annex II del RD 3/2010:
• Anàlisi i Gestió de riscos.

• Tipus de proves: sustentació metodològica de l'anàlisi de riscos realitzat, la seva coherència i documentació, i verificació de l'inventari de actius. Per això l'equip auditor pot basar-se en la norma UNE 71.504
- Metodologia d'anàlisi i gestió de riscos dels sistemes de informació. En aquest apartat no és d'aplicació la selecció de mostres.

• El marc organitzatiu i la segregació de funcions.
• Tipus de proves: documentació de les polítiques i procediments (Accessibilitat pel personal a què afecta i actualització); la comunicació de les normes, de les responsabilitats i de la conscienciació del personal afectat sobre aquestes normes, polítiques i procediments. Es recomana que als efectes d'una avaluació més representativa, s'entrevisti no només a càrrecs jeràrquics, sinó també a altre personal de forma aleatòria.

• El marc operacional (Control d'Accessos, Explotació, Serveis Externs, Continuïtat del Servei, i Monitorització del Sistema).
• Tipus de proves: avaluació, entre d'altres, de les proves fefaents de la continuïtat del servei, amb inclusió o no dels serveis externs; les autoritzacions i sol·licituds d'accés, el registre i seguiment dels incidents de seguretat; l'adequació dels drets d'accés que considerin la segregació de funcions, avaluació del control de capacitat dels sistemes, els mecanismes de control per a l'accés físic, etc.

• La Declaració de Aplicabilitat que recull les mesures de seguretat de l'Annex II que són rellevants per al sistema d'informació subjecte a l'auditoria.
• Així mateix, si es realitza una auditoria simultània segons els requisits del RD 1720/2007, cal que els auditors identifiquin les mesures establertes pel compliment específic d'aquesta norma.
• Tipus de proves: la revisió dels registres d'activitat, la seva revisió i supervisió; fortalesa de les mesures de seguretat de les comunicacions enfront d'atacs interns o externs, control de canvis en aplicacions i sistemes, compliment de contractes de propietat intel·lectual, etc.

• Els processos de millora contínua de la seguretat.
• Tipus de proves: avaluar el cicle de maduresa del sistema de gestió de la seguretat del sistema d'informació auditat, criteris per a la revisió i agenda de millores.

• L'aplicació dels models de clàusula administrativa particular a incloure en les prescripcions administratives dels contractes corresponents (segons una mostra seleccionada d'aquests).

Per a definir la tipologia de proves a realitzar (verificació de les mesures de seguretat), l'equip auditor pot utilitzar guies, i qüestionaris d'auditoria disponibles a associacions i col·lectius d'auditors, i les guies STIC proporcionades pel CCN que siguin d'aplicació al sistema auditat. Aquestes guies poden ser una bona base per a, dins de l'abast de l'auditoria, dissenyar proves adequades, mantenint sempre un criteri analític i de proporcionalitat. A l'Annex I s'inclouen referències d'aquestes guies.

El cap de l'equip auditor ha de valorar quina informació o documentació és necessària sol·licitar al començament de l'auditoria, per assegurar que es té una fotografia fidel de determinades mesures de seguretat al començament de la mateixa, com poden ser, entre altres possibles i segons es consideri aplicable:

• Llista del personal que ha deixat l'organisme recentment.
• Còpia del registre d'incidències
• Còpia del registre d'activitat dels usuaris
• Registres de formació del personal afectat pel sistema auditat.

Aquest tipus d'evidències pot assistir a l'auditor en l'avaluació de si determinades mesures de seguretat s'han realitzat consistent i homogèniament.

Durant la definició de les proves a realitzar, es valorarà si cal demanar comptes d'accés al sistema auditat per a alguns integrants de l'equip auditor.

3.5. REVISIONS I PROVES D'AUDITORIA

Per a la realització de les proves d'auditoria, l'auditor tindrà en compte com a normes generals, les següents premisses:
• La planificació de les proves a realitzar, especialment les d'observació i proves tècniques, és un element privatiu de l'equip auditor. Per tant, aquest no té obligació de anticipar-les al personal auditat, excepte pel que fa a la agenda o disponibilitat d'elements per a l'execució de la prova.
• En la realització de determinades proves com la verificació documental de autoritzacions, aprovacions o contractes, l'auditor podrà requerir la revisió dels documents. Aquests documents, bé en suport electrònic o en paper, podran ser originals o constituir algun dels tipus de còpia previstos a les Normes Tècniques d'Interoperabilitat, en relació a l'evidència a la qual hagin de servir a efectes de verificació (per exemple, en el cas en què, determinat document, pugui servir com a evidència d'una conclusió a incorporar a l'informe d'auditoria).
• La mostra seleccionada de mesures o documentació ha de ser suficient i rellevant per satisfer del compliment objectiu de la prova, dins de l'abast i objectiu de l'auditoria. El cap de l'equip d'auditoria pot decidir que s'ampliï la mostra si considera que la mida d'aquesta no és suficient.
• L'equip auditor no prejutja, a priori, en l'existència de determinades mesures, ni serà inflexible en la seva funcionalitat. En avaluar les mesures existents haurà sempre considerar, objectivament, si s'ajusten al que preveu pel RD 3/2010 i si prevenen realment els riscos identificats en l'Anàlisi de Riscos.
• Davant l'absència de determinada mesura, s'investigarà i analitzarà si hi ha altres mesures compensatòries, i si escau, s'avaluarà l'eficàcia d'aquestes últimes.
• Les entrevistes no es plantejaran de manera inductiva (conduir a una contestació concreta), sinó obertes (com es realitza determinada activitat o es concreta en la pràctica determinada mesura de seguretat). És a dir: no s'han de realitzar preguntes on la resposta, afirmativa o negativa segons el cas, estigui implícita en la pregunta.
• Es ponderaran les respostes de les entrevistes, podent haver lloc a la realització de proves complementàries que no estaven previstes.

Per a les evidències de les proves l'auditor tindrà en compte com a normes generals, les següents:
• El cap de l'equip auditor haurà de supervisar tota la feina feta i comprovar que s'ha dut a terme el programa d'auditoria previst i aprovat, i que les desviacions al programa, o les seves modificacions, estan degudament fonamentades, i registrades.
• L'evidència recollida ha de ser suficient i rellevant perquè:
o si no hi ha incidències a comunicar, s'acrediti la realització adequada de la prova i els seus resultats.

o si hi ha incidències a incloure en l'informe, es sustenti clarament el incompliment persistent o una indiscutible deficiència de seguretat, i no aquelles situacions excepcionals o puntuals, si estan reportades, controlades, i aprovades, llevat que l'excepcionalitat no hauria d'haver estat aprovada, pel risc que pogués implicar, segons el judici objectiu i sustentat l'auditor.
• La revisió de documentació (incloent l'anàlisi de riscos) haurà documentar amb les conclusions de la revisió, i les possibles aclariments rebudes posteriorment.
• Les conclusions o informació recollida en una entrevista, per poder ser considerades com a evidències d'auditoria, hauran de ser plasmades en actes comunicades a les persones entrevistades.
• Els correus electrònics, en la mesura que involucri a diverses persones dins el abast de l'auditoria, i es disposi del justificant de recepció, poden servir, en determinats casos, també com a prova d'auditoria.
• Les proves d'observació (per exemple seguretat física) hauran d'estar documentades ja sigui a través de fotografies, documentació similar, o comunicacions escrites puntuales2 al Responsable de Seguretat.
• Les evidències que es recullin han d'evitar, en la mesura possible, contenir dades de caràcter personal, o si cal com a evidència, que els continguin, s'ha d'utilitzar algun mecanisme (supressió, ratllat, etc.) que impedeixi la seva divulgació.
• Les evidències que calgui presentar a requeriment de qui tingui competències per sol·licitar-les, hauran acollir-se a la pràctica habitual i en particular, si es tracta d' evidències electròniques, s'han de sotmetre a les Normes Tècniques de Interoperabilitat que siguin aplicables.
• Els documents de treball de l'auditor (planificació, documentació revisada, evidències, actes de reunions, llistats, còpies de pantalles, i evidències similars del treball realitzat, ja siguin en suport paper o electrònic) s'han de mantenir com mínim durant els dos següents anys, degudament referenciats i arxivats, així com custodiats i protegits.

3.6. ELABORACIÓ I PRESENTACIÓ DELS RESULTATS DE REVISIONS I PROVES D'AUDITORIA

L'objectiu principal de la presentació dels resultats de les revisions i proves, abans de l'emissió de l'informe d'auditoria, és confirmar els fets i les situacions detectades o identificades com a resultat de les proves i revisions realitzades. Aquesta presentació tindrà un caràcter asèptic, sense valoracions subjectives, ni al·ludint a la valoració dels resultats finals a plasmar en l'informe, que és l'opinió professional l'auditor.

Aquesta presentació és fonamental per a l'eficàcia de l'informe d'auditoria posterior, al confirmar que els resultats, de les revisions i les proves, són certes, i que no existeix altra informació, que per no haver estat considerada o no ser-hi en el seu moment, podria canviar l'avaluació del compliment de determinat requisit de seguretat.

Tots els resultats de proves, relacionats entre si o que facin referència a una mateixa deficiència o debilitat, seran agrupats per l'informe, tot i que s'inclogui un detall de les deficiències de forma individual, en un annex a l'Informe d'Auditoria.

En relació als requisits del Títol VIII del RD 1720/2007, quan hi hagi una divergència contrastable entre l'aplicació d'aquests i els del RD 3/2010, resultant un incompliment del primer, s'ha d'indicar amb claredat aquesta situació, ja que els requisits del RD 1720/2007 són

prioritaris, com a desenvolupament d'una llei orgànica (Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal).

Si bé l'objectiu principal és la verificació del compliment acceptable del RD 3/2010, l'equip auditor ha de tenir en compte que aquests requisits són mínims i per tant, si observa alguna deficiència que pot implicar riscos en la protecció de la informació, haurà de comunicar.

3.7. PRESENTACIÓ DE L'INFORME D'AUDITORIA

42. Un cop confirmats els fets i deficiències resultats de les revisions i proves de auditoria, aquest informe haurà de presentar-se al Responsable del Sistema i al Responsable de Seguretat. Segons el RD 3/2010 els informes d'auditoria seran analitzats pel responsable de seguretat competent, que elevarà les conclusions al responsable del sistema perquè adopti les mesures correctores adients.

L'equip auditor no lliurarà ni concedirà accés a l'informe d'auditoria a tercers diferents dels indicats en el paràgraf anterior, llevat per imperatiu legal o mandat judicial.

L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures exigides pel RD 3/2010, identificar-ne les deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, fets i observacions en què es basin els dictàmens i les recomanacions propostes.

L'informe inclourà les no conformitats trobades durant la realització de la auditoria

L'informe inclourà una opinió sobre si:
• La Política de Seguretat defineix els rols i funcions dels responsables de la informació, els serveis, els actius i la seguretat del sistema de informació.
• Hi ha procediments per a la resolució de conflictes entre aquests responsables.
• S'han designat persones per a aquests rols a la llum del principi de "Separació de funcions".
• Hi ha un sistema de gestió de la seguretat de la informació, documentat i amb un procés regular d'aprovació per la direcció.
• S'ha realitzat una anàlisi de riscos, amb revisió i aprovació regular, segons el que estableix les mesures aplicables de l'annex II del RD 3/2010.
• Es compleixen les mesures de seguretat descrites en l'Annex II, sobre Mesures de Seguretat, en funció de les condicions d'aplicació en cada cas.
• Hi ha un sistema de gestió de millora contínua.
• Si l'auditoria es realitzés conjuntament amb la requerida pel RD 1720/2007 en els seus articles 96 i 110, cal que l'informe indiqui amb claredat quan una deficiència de seguretat o incompliment, o una millora recomanada està, individualment, relacionada amb les dues normes, o bé amb una en concret.

L'Informe d'Auditoria es pot presentar en format audiovisual. Tanmateix, aquest informe sempre s'ha de lliurar en suport paper i degudament signat, o bé en suport electrònic amb signatura electrònica. L'esquema de l'informe inclourà com mínim:
• Data d'emissió de l'informe
• Una secció d'abast, limitacions a l'abast, i objectiu de l'auditoria, amb la deguda identificació del sistema auditat.
• Breu descripció del procés metodològic aplicat per realitzar la auditoria.
• Identificació de la documentació revisada.

• Identificació de la tipologia de proves realitzades.
• Les dates (de començament i final del treball de camp, ja siguin reunions com revisions tècniques) en què s'ha realitzat el treball d'auditoria
• Indicació de si hi ha hagut alguna limitació en la realització de les proves o revisions, que impedeixin donar una opinió sobre determinats elements de seguretat.
• Una secció d'informe executiu resumint els aspectes més rellevants o les àrees d'acció més significatives, amb un resum general del grau de compliment.
• Les recomanacions en cap cas han de ser tancades, sinó suggeriments de les diferents alternatives possibles, quan sigui aplicable, a considerar pels responsables de seguretat.
• Les recomanacions estaran sempre basades en l'existència d'un risc i sustentades degudament, o bé relacionades amb un incompliment fefaent i precís dels requisits bàsics i mínims del RD 3/2010.
• En annexos es podran descriure els detalls i resultats de les proves que permeten arribar a les conclusions de l'informe executiu, agrupant-los pels apartats de l'informe executiu.
• L'informe també podrà incloure com a annex les contestacions del Responsable de seguretat als comentaris abocats en l'informe, o les accions que es prendran per solucionar les deficiències, si n'hi ha.
• L'Informe d'Auditoria ha de ser signat pel Cap de l'equip d'auditoria, i indicar els participants en l'equip d'auditoria en un annex o a continuació de la signatura del Cap de l'equip.

En l'informe executiu no s'inclouran termes o acrònims informàtics, ja que el informe podrà ser llegit per directors i gerents, o tercers, que no tinguin el coneixement informàtic adequat. Tampoc s'hauran d'incloure noms de persones concretes, només funcions o llocs exercits.

ANNEX 4: DECLARACIÓ D'APLICABILITAT

ÍNDEX

INTRODUCCIÓ

L'objectiu del present document és definir què controls són adequats per implementar en l'organització, quins són els objectius d'aquests controls i com s'implementen. També té com a objectiu aprovar riscos residuals i aprovar formalment la implementació dels controls esmentats.

NIVELLS DE MADURESA

Aquesta valoració la realitzarem segons el Model de Maduresa de la Capacitat (CMM):

OBJECTIUS I PUNTS DE CONTROL

En compliment de l'Esquema Nacional de Seguretat, els objectius i punts de control seran els que defineix aquest, per tant:

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

Com a complement, s'avaluaran els punts de control de l'ISO 27002:

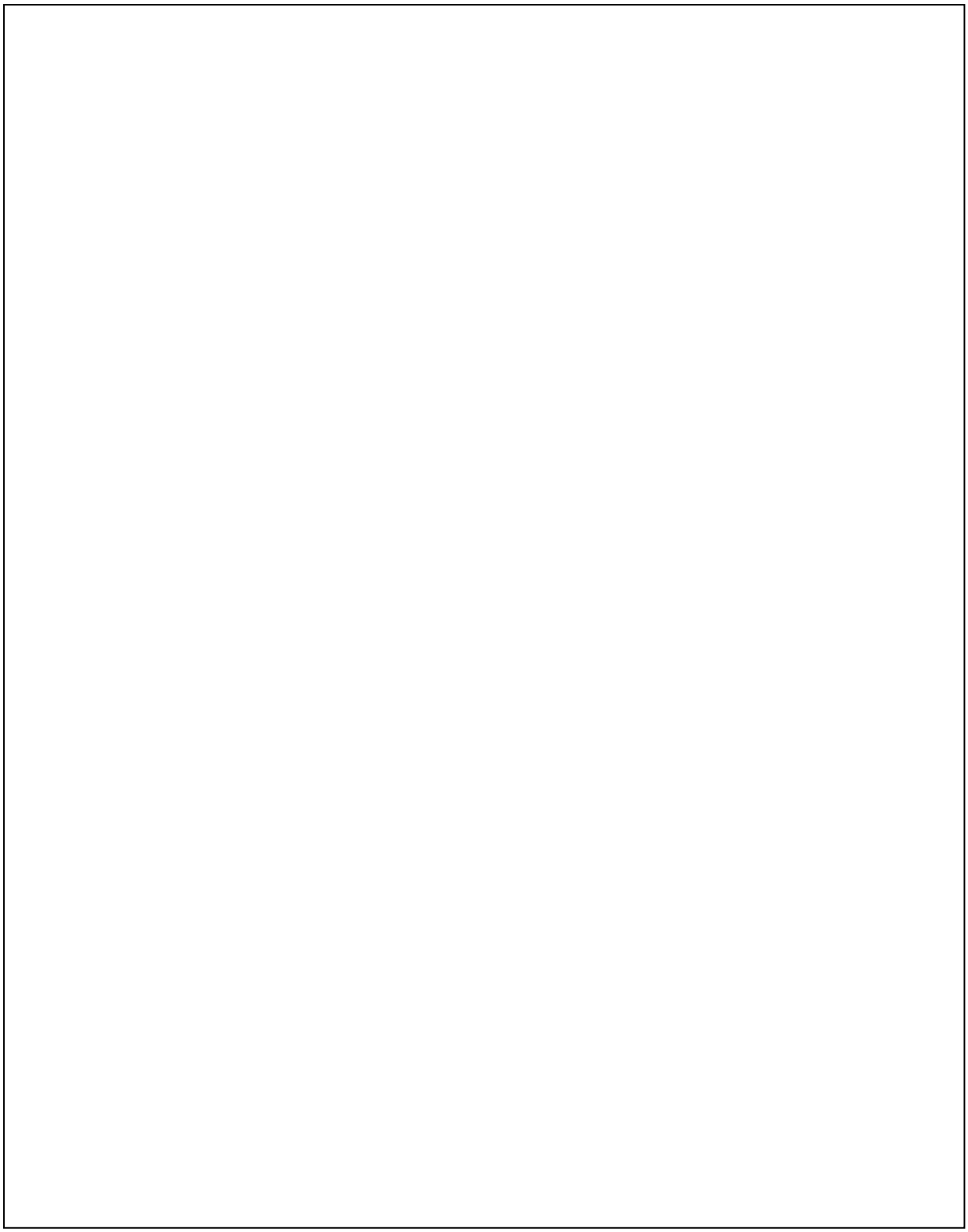
5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de Activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y Activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓ
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las Aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓ.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ANNEX 5: Organigrama



Annex 6: Auditoria de compliment ISO 27002:2013

Autora: Verónica Alejaldre García
Data: 16/12/2016

CONTROL DE VERSIONS

Versió	Motiu	Data publicació
1	Creació	16/12/2016

Índex

1. Objectiu

El present document té com a objectiu plasmar la informació obtinguda a través d'un procés d'auditoria per tal d'avaluar la maduresa de la seguretat, pel que fa als diferents dominis de control plantejats per la ISO/IEC 27002:2013.

2. Abast

L'abast d'aquesta auditoria inclou totes les dependències de l'organització en les quals es disposa d'equipament informàtic, així com qualsevol persona o empresa que tingui o pugui tenir contacte amb aquest.

3. Normativa de referència

Com a normativa de referència es prendrà l'estàndard ISO/IEC 27002:2013, el qual agrupa un total de 113 controls o mesures preventives sobre "bones pràctiques" per a la Gestió de la Seguretat de la Informació, organitzats en 14 àrees i 35 objectius de control. Aquest estàndard es internacionalment reconegut i es perfectament vàlid per a la majoria de les organitzacions.

4. Metodologia i temporalització

La metodologia de treball emprada per a la realització d'aquest document ha estat la següent:

Definició	**Descripció**	**Temporalitzacio**
Recol·lecció d'informació prèvia	Reunions amb els diferents interlocutors designats per l'empresa i recull de dades tècniques necessàries	3 dies
Execució de les proves d'auditoria		
Proves tècniques	Realització de les proves	15 dies
Visites	Visites a les instal·lacions per comprovar la seguretat física	10 dies
Entrevistes	Entrevistes amb el personal implicat en els sistemes per verificar que coneixen i apliquen les polítiques de seguretat	7 dies

5. Llista detallada de punts de control

Per tal d'avaluar els controls continguda en la ISO 27002:2013, realitzarem la valoració segons la següent taula, que es basa en el Model de Maduresa de la Capacitat (CMM):

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem. No s'ha reconegut que existeixi cap problema a resoldre.
10%	L1	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. Els procediments son inexistents o localitzats en àrees concretes. No existeixen plantilles
50%	L2	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca. Es normalitzen les "bones practiques" en base a l'experiència i al mètode. No hi ha comunicació o entreteniment formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	L3	Procés definit	La organització sencera participa al procés. Els processos estan implantats, documentats i comunicats mitjançant entreteniment.
95%	L4	Gestionat y mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, s'ha de tenir eines per a millorar la qualitat i la eficiència.
100%	L5	Optimitzat	Els processos estan sota constant millora. En base criteris quantitatius es determinen les desviacions

Així, a continuació es detallen aquests punts de control:

Control	EFECTIVITAT
5. POLÍTICAS DE SEGURIDAD.	**90%**
5.1 Directrices de la Dirección en seguridad de la información.	90%
5.1.1 Conjunto de políticas para la seguridad de la información.	90%
5.1.2 Revisión de las políticas para la seguridad de la información.	90%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	**90%**

Control	EFECTIVITAT
6.1 Organización interna.	90%
6.1.1 Asignación de responsabilidades para la segur. de la información.	90%
6.1.2 Segregación de tareas.	90%
6.1.3 Contacto con las autoridades.	90%
6.1.4 Contacto con grupos de interés especial.	90%
6.1.5 Seguridad de la información en la gestión de proyectos.	90%
6.2 Dispositivos para movilidad y teletrabajo.	90%
6.2.1 Política de uso de dispositivos para movilidad.	90%
6.2.2 Teletrabajo.	90%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**90%**
7.1 Antes de la contratación.	90%
7.1.1 Investigación de antecedentes.	90%
7.1.2 Términos y condiciones de contratación.	90%
7.2 Durante la contratación.	90%
7.2.1 Responsabilidades de gestión.	90%
7.2.2 Concienciación, educación y capacitación en segur. de la informac.	90%
7.2.3 Proceso disciplinario.	9%
7.3 Cese o cambio de puesto de trabajo.	90%
7.3.1 Cese o cambio de puesto de trabajo.	90%
8. GESTIÓN DE ACTIVOS.	**90%**
8.1 Responsabilidad sobre los Activos.	90%
8.1.1 Inventario de Activos.	90%
8.1.2 Propiedad de los Activos.	90%
8.1.3 Uso aceptable de los Activos.	90%
8.1.4 Devolución de Activos.	90%
8.2 Clasificación de la información.	90%
8.2.1 Directrices de clasificación.	90%
8.2.2 Etiquetado y manipulado de la información.	90%
8.2.3 Manipulación de Activos.	90%
8.3 Manejo de los soportes de almacenamiento.	90%
8.3.1 Gestión de soportes extraíbles.	90%
8.3.2 Eliminación de soportes.	90%
8.3.3 Soportes físicos en tránsito.	90%
9. CONTROL DE ACCESOS.	**90%**
9.1 Requisitos de negocio para el control de accesos.	90%
9.1.1 Política de control de accesos.	90%

Control	EFECTIVITAT
9.1.2 Control de acceso a las redes y servicios asociados.	90%
9.2 Gestión de acceso de usuario.	90%
9.2.1 Gestión de altas/bajas en el registro de usuarios.	90%
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	90%
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	90%
9.2.4 Gestión de información confidencial de autenticación de usuarios.	90%
9.2.5 Revisión de los derechos de acceso de los usuarios.	90%
9.2.6 Retirada o adaptación de los derechos de acceso	90%
9.3 Responsabilidades del usuario.	90%
9.3.1 Uso de información confidencial para la autenticación.	90%
9.4 Control de acceso a sistemas y Aplicaciones.	90%
9.4.1 Restricción del acceso a la información.	90%
9.4.2 Procedimientos seguros de inicio de sesión.	90%
9.4.3 Gestión de contraseñas de usuario.	90%
9.4.4 Uso de herramientas de administración de sistemas.	90%
9.4.5 Control de acceso al código fuente de los programas.	90%
10. CIFRADO.	**90%**
10.1 Controles criptográficos.	90%
10.1.1 Política de uso de los controles criptográficos.	90%
10.1.2 Gestión de claves.	90%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	**90%**
11.1 Áreas seguras.	90%
11.1.1 Perímetro de seguridad física.	90%
11.1.2 Controles físicos de entrada.	90%
11.1.3 Seguridad de oficinas, despachos y recursos.	90%
11.1.4 Protección contra las amenazas externas y ambientales.	90%
11.1.5 El trabajo en áreas seguras.	90%
11.1.6 Áreas de acceso público, carga y descarga.	90%
11.2 Seguridad de los equipos.	90%
11.2.1 Emplazamiento y protección de equipos.	90%
11.2.2 Instalaciones de suministro.	90%
11.2.3 Seguridad del cableado.	90%
11.2.4 Mantenimiento de los equipos.	90%
11.2.5 Salida de Activos fuera de las dependencias de la empresa.	90%
11.2.6 Seguridad de los equipos y Activos fuera de las instalaciones.	90%
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	90%

Control	EFECTIVITAT
11.2.8 Equipo informático de usuario desatendido.	90%
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	90%
12. SEGURIDAD EN LA OPERATIVA.	**90%**
12.1 Responsabilidades y procedimientos de operación.	90%
12.1.1 Documentación de procedimientos de operación.	90%
12.1.2 Gestión de cambios.	90%
12.1.3 Gestión de capacidades.	90%
12.1.4 Separación de entornos de desarrollo, prueba y producción.	90%
12.2 Protección contra código malicioso.	90%
12.2.1 Controles contra el código malicioso.	90%
12.3 Copias de seguridad.	90%
12.3.1 Copias de seguridad de la información.	90%
12.4 Registro de actividad y supervisión.	90%
12.4.1 Registro y gestión de eventos de actividad.	90%
12.4.2 Protección de los registros de información.	90%
12.4.3 Registros de actividad del administrador y operador del sistema.	90%
12.4.4 Sincronización de relojes.	90%
12.5 Control del software en explotación.	90%
12.5.1 Instalación del software en sistemas en producción.	90%
12.6 Gestión de la vulnerabilidad técnica.	90%
12.6.1 Gestión de las vulnerabilidades técnicas.	90%
12.6.2 Restricciones en la instalación de software.	90%
12.7 Consideraciones de las auditorías de los sistemas de información.	90%
12.7.1 Controles de auditoría de los sistemas de información.	90%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	**90%**
13.1 Gestión de la seguridad en las redes.	90%
13.1.1 Controles de red.	90%
13.1.2 Mecanismos de seguridad asociados a servicios en red.	90%
13.1.3 Segregación de redes.	90%
13.2 Intercambio de información con partes externas.	90%
13.2.1 Políticas y procedimientos de intercambio de información.	90%
13.2.2 Acuerdos de intercambio.	90%
13.2.3 Mensajería electrónica.	90%
13.2.4 Acuerdos de confidencialidad y secreto.	90%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓ	**90%**
14.1 Requisitos de seguridad de los sistemas de información.	90%

Control	EFECTIVITAT
14.1.1 Análisis y especificación de los requisitos de seguridad.	90%
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	90%
14.1.3 Protección de las transacciones por redes telemáticas.	90%
14.2 Seguridad en los procesos de desarrollo y soporte.	-
14.2.1 Política de desarrollo seguro de software.	-
14.2.2 Procedimientos de control de cambios en los sistemas.	-
14.2.3 Revisión técnica de las Aplicaciones tras efectuar cambios en el sistema operativo.	-
14.2.4 Restricciones a los cambios en los paquetes de software.	-
14.2.5 Uso de principios de ingeniería en protección de sistemas.	-
14.2.6 Seguridad en entornos de desarrollo.	-
14.2.7 Externalización del desarrollo de software.	-
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	-
14.2.9 Pruebas de aceptación.	-
14.3 Datos de prueba.	-
14.3.1 Protección de los datos utilizados en pruebas.	-
15. RELACIONES CON SUMINISTRADORES.	**90%**
15.1 Seguridad de la información en las relaciones con suministradores.	90%
15.1.1 Política de seguridad de la información para suministradores.	90%
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	90%
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	90%
15.2 Gestión de la prestación del servicio por suministradores.	90%
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	90%
15.2.2 Gestión de cambios en los servicios prestados por terceros.	90%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓ.	**90%**
16.1 Gestión de incidentes de seguridad de la información y mejoras.	90%
16.1.1 Responsabilidades y procedimientos.	90%
16.1.2 Notificación de los eventos de seguridad de la información.	90%
16.1.3 Notificación de puntos débiles de la seguridad.	90%
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	90%
16.1.5 Respuesta a los incidentes de seguridad.	90%
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	90%
16.1.7 Recopilación de evidencias.	90%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**90%**

Control	EFECTIVITAT
17.1 Continuidad de la seguridad de la información.	90%
17.1.1 Planificación de la continuidad de la seguridad de la información.	90%
17.1.2 Implantación de la continuidad de la seguridad de la información.	90%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	90%
17.2 Redundancias.	90%
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	90%
18. CUMPLIMIENTO.	**90%**
18.1 Cumplimiento de los requisitos legales y contractuales.	90%
18.1.1 Identificación de la legislación aplicable.	90%
18.1.2 Derechos de propiedad intelectual (DPI).	90%
18.1.3 Protección de los registros de la organización.	90%
18.1.4 Protección de datos y privacidad de la información personal.	90%
18.1.5 Regulación de los controles criptográficos.	90%
18.2 Revisiones de la seguridad de la información.	90%
18.2.1 Revisión independiente de la seguridad de la información.	90%
18.2.2 Cumplimiento de las políticas y normas de seguridad.	90%
18.2.3 Comprobación del cumplimiento.	90%

6. No conformitats

Com a resultat de l'auditoria s'han trobat un total de 4 no conformitats, detallades a continuació:

Control	CONFORMITAT
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	No conformitat
7.3 Cese o cambio de puesto de trabajo.	
7.3.1 Cese o cambio de puesto de trabajo.	No conformitat
8. GESTIÓN DE ACTIUS.	
8.1.4 Devolución de activos.	No conformitat
11. SEGURIDAD FÍSICA Y AMBIENTAL.	
11.1 Áreas seguras.	
11.1.2 Controles físicos de entrada.	No conformitat

7. Millores

De manera general cal incorporar procediments que permetin assolir un següent nivell de maduresa en els controls avaluats, de manera que es pugui seguir amb indicadors numèrics i estadístics l'evolució dels processos disposar de tecnologia per automatitzar el flux de treball i tenir eines per a millorar la qualitat i la eficiència.

Pel que fa a les no conformitats:

1. Cal sol·licitar referències al possible nou personal i contrastar-les
2. Cal notificar del cessament en el lloc de treball a les àrees afectades i prendre les mesures de seguretat establertes en les polítiques de seguretat.
3. Cal revisar els actius en el moment de les devolucions, i registrar correctament el retorn, degut al volum de feina no sempre es fa.
4. El control físic d'accés durant l'horari d'oficina no es realitza, de manera que els visitants accedeixen als espais fins que algú els hi pregunta. Cal limitar aquest accés de manera segura.

8. Resum executiu

En relació a l'objecte d'aquesta auditoria, un cop completada, es por concloure que, en general, els procediments establerts s'estan realitzant correctament i garanteixen el nivell d'efectivitat detallat a l'apartat de constatacions, però, s'ha de solucionar les 4 no conformitats trobades i detallades al punt anterior.