Plan Director de Seguridad en la Administración Local bajo la perspectiva de la Calidad del Dato.

Nombre Estudiante: Ramón Asensio Palao

Programa: Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 28 de Diciembre de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Plan Director de Seguridad en la Administración Local bajo la perspectiva de la Calidad del Dato.*
Nombre del autor:	*Ramón Asensio Palao*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2020
Titulación::	Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	***Castellano***
Palabras clave	*ENS, ISO 27001, ENI, ISO 25012, SGSI*

Resumen del Trabajo*:*

Trabajo práctico para implantar un Plan Director de Seguridad en una Administración Pública Local española bajo el amparo de estándares como el Esquema Nacional de Seguridad (ENS) e ISO/IEC 27001 pero sin olvidar la calidad del dato ni su interoperabilidad. Se crea una nueva metodología sencilla de aplicación sobre ISO 25012 con el fin de encontrar ese equilibrio que nos permita tener sistemas de información seguros y también útiles. Se aborda una implantación del ENS condicionada por ISO 25012 para posteriormente ir acercándonos a ISO/IEC 27001 y conseguir las ventajas de los tres estándares.

Se desarrolla toda la documentación principal necesaria, se realiza un análisis de riesgos con metodología MAGERIT, proponemos proyectos de mejora de la seguridad sobre el sistema de información sustituyendo aquellas partes que no cumplan con los objetivos de calidad del dato y realizamos una auditoría para evaluar el cumplimiento de las normativas.

Nuestra aproximación desde el ENS hacia ISO/IEC 27001 nos ha permitido priorizar aquellos proyectos de elevado riesgo contando siempre con la aprobación de la dirección de la administración, hemos conseguido mejorar la seguridad en ambos estándares si bien es cierto que se ha avanzado más en ENS que en ISO/IEC 27001 es debido al tipo de aproximación realizada por tratarse de un ente público. El cribado de proyectos ISO/IEC 25012 nos ha permitido no invertir recursos en la parte del sistema que es mejor sustituir antes que securizar y ha conseguido poner al ciudadano en el centro de la administración electrónica.

Abstract:

Practical work to implement a Security Master Plan in a Spanish Local Public Administration under the protection of standards such as the National Security Scheme (ENS) and ISO/IEC 27001, while considering the quality of the data and its interoperability. A new simple application methodology on ISO 25012 is created to find a balance that allows us to have secure and applicable information systems. An implementation of the ENS conditioned by ISO 25012 is approached to later move closer to ISO/IEC 27001 and obtain the advantages of the three standards.

We develop all the necessary main documentation, a risk analysis is carried out using MAGERIT methodology, we propose projects to improve the security of the information system by substituting those parts that do not meet the data quality objectives and we carry out an audit to evaluate the compliance with regulations.

Our approach from ENS to ISO/IEC 27001 has allowed us to prioritize those high risk projects, always assuming the approval of the administration's high direction, we have managed to improve security in both standards although more progress has been made in ENS than in ISO/IEC 27001, due to the type of approach made for a public entity. The screening of ISO 25012 projects has enabled us to not invest resources in parts of the system that are better replaced than secured, and has managed to put the citizen at the center of electronic administration.

Índice

Lista de figuras

Índice de tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

En el Digital Enterprise Show de 2019 celebrado en Madrid, Carlos Escudero, gerente de informática de la Seguridad Social española, expuso como en el nuevo gobierno del dato en la Administración Pública antiguamente tenía prioridad la normativa frente al ciudadano y en la actualidad esta tendencia se ha invertido para dar prioridad al ciudadano sobre la normativa. En este mismo foro Unai Martín, subdirector adjunto de la subdirección general de aplicaciones del departamento de informática para la Agencia Tributaria apoyaba la prioridad del contribuyente sobre la normativa y abogaba por el suministro inmediato de información. Finalmente Maria Jesús Villamediana gerente de Informática del Ayuntamiento de Madrid (IAM) ponía nuevamente al ciudadano en el epicentro del dato y defendía la disponibilidad de la información en dispositivos móviles.

Es tendencia entre los dirigentes TIC de la Administración Pública la implantación de nuevas tecnologías basadas en el Big Data, IOT, Business Intelligence, etc. que se apoyan en la calidad del dato y cuyo fin último es poner al ciudadano en el centro del nuevo gobierno del dato. Según ISO/IEC 25012 la calidad de datos se compone de las siguientes características:

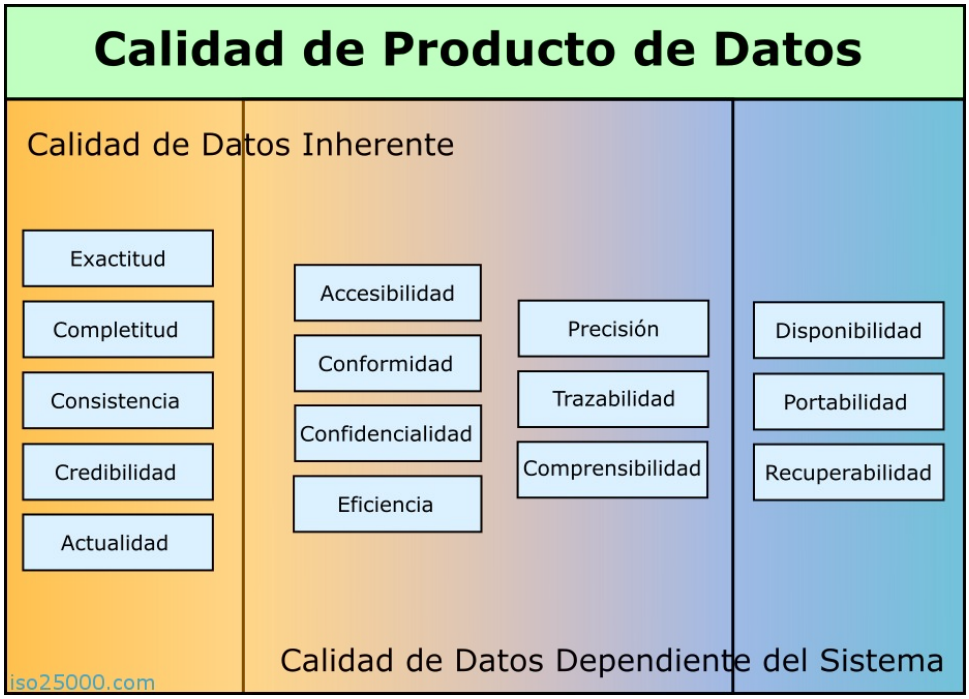

Figura 1 - ISO 25012 [32]

Como podemos observar en la figura 1 tanto ISO/IEC 27001 como ISO/IEC 25012 tienen objetivos comunes en los pilares básicos de la información: disponibilidad, integridad y confidencialidad.

Los sistemas de gestión de seguridad de la información (en adelante SGSI) tienen que buscar este mismo objetivo en un juego de suma no nula donde ambas partes salgan beneficiadas, dando al ciudadano máxima prioridad a la hora de ofrecer servicios en muchas ocasiones críticos pero manteniendo unos niveles de seguridad de la información adecuados. Securizaremos sistemas que busquen la calidad del dato en lugar de buscar la calidad del dato en sistemas seguros, en caso de advertir la presencia de sistemas inseguros que no respeten la calidad del dato se priorizará su cambio sobre su posible securización evaluando siempre la criticidad de la decisión.

Este trabajo buscará desarrollar un Plan Director de Seguridad para una administración local, basado en el estándar internacional ISO/IEC 27001 y en la norma estatal del Esquema Nacional de Seguridad de obligado cumplimiento para las Administraciones Públicas pero buscando un equilibrio con otras normas como ISO/IEC 25012, ISO/IEC 27002, el RGPD, la LOPDGDD o el Esquema Nacional de Interoperabilidad, permitiendo que todos los servicios prestados giren entorno al ciudadano. También acercaremos posturas entre la dirección de la organización y el departamento TIC con el Responsable de Seguridad como nexo de unión.

1.2. Objetivos del Trabajo

- Mejorar la seguridad del sistema integral de gestión de información de una administración pública local.
- Dar cumplimiento a las normativas de Esquema Nacional de Seguridad y Esquema Nacional de Interoperabilidad.
- Implementar buenas prácticas en los SGSI acordes a ISO/IEC 27001 e ISO/IEC 27002.
- Establecer nexos de unión entre seguridad y calidad del dato.
- Acercar el gobierno del dato al ciudadano.
- Convertir este TFM en una guía práctica de cumplimiento de ENS y Calidad del Dato aplicable a la Administración Local.

1.3. Enfoque y método seguido

El método seguido constará de 6 fases estructuradas del siguiente modo:

Fase 1. Contextualización, objetivos y análisis diferencial. Introducción al proyecto. Enfoque y selección de empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis Diferencial de la empresa con respecto al ENS, al ENI, ISO/IEC 27001 e ISO/IEC 27002. Establecer el alcance de la evaluación de la calidad del dato.

Fase 2. Sistema de Gestión Documental. Elaboración Política de Seguridad. Declaración de aplicabilidad y Documentación del SGSI. Elaboración del Plan de Calidad del Dato.

Fase 3. Análisis de riesgos. Elaboración de una metodología de análisis de riesgos empleando MAGERIT: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual. Elaboración de una metodología de la calidad del dato: Identificación y valoración de activos importantes en la calidad del dato, nivel de calidad del dato aceptable.

Fase 4. Propuesta de proyectos. Evaluación de proyectos que debe llevar a cabo la organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

Fase 5. Auditoría de cumplimiento de Esquema Nacional de Seguridad y buenas prácticas de ISO/IEC 27002:2013. Evaluación de los controles, madurez y nivel de cumplimiento una vez aplicadas las propuestas de la Fase 4. Exposición de hallazgos.

Fase 6. Presentación de Resultados y entrega de Informes. Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a la Dirección. Entrega del proyecto final.

Este enfoque no busca llevar a cabo un análisis de la calidad del dato y de la seguridad de la información de un modo independiente, por esto empleamos sólo seis fases en lugar de desplegar cada una de ellas para cada perspectiva. Se ha elegido MAGERIT por ser desarrollado en España y contar con numerosa documentación y herramientas de adecuación al Esquema Nacional de Seguridad. En la evaluación de la calidad del dato se emplearán pruebas piloto aún en fase experimental.

1.4. Planificación del Trabajo

Fase 1.
Plazo para conseguirlo: del 26-09 al 4-10
Hitos a conseguir:
- Planificación Inicial del Trabajo de Final de Máster (2 días)
- Descripción detallada de la Administración Local (1 día)
- Objetivos del Plan Director (0,25 día)
- Alcance del Plan Director de Seguridad (0,25 día)
- Objetivos en la Evaluación de la Calidad del Dato (0,25 día)
- Alcance en la Evaluación de la Calidad del Dato (0,25 día)
- Análisis diferencial (2 días)

TOTAL: 6 DÍAS

Fase 2.
Plazo para conseguirlo: del 5-10 al 16-10
Hitos a conseguir:
- Revisión de Fase 1 (1 día)
- Política de Seguridad (2 día)
- Procedimiento de Auditorías Internas (2 día)

- Gestión de Indicadores (0.25 día)
- Procedimiento de Revisión por Dirección (0.5 día)
- Gestión de Roles y Responsabilidades (0.5 día)
- Metodología de Análisis de Riesgos (0.25 día)
- Declaración de Aplicabilidad (1 día)
- Plan de Calidad del Dato (1 día)

TOTAL: 9 DÍAS

Fase 3.
Plazo para conseguirlo: del 17-10 al 6-11.
Hitos a conseguir:
- Revisión de Fase 2 (1 día)
- Inventario y dependencias de Activos (1 día)
- Valoración de los Activos y valoración ACIDA (2 días)
- Identificación de activos para evaluar su calidad del dato (0,5 día)
- Valoración de la calidad del dato (0,5 día)
- Análisis de Amenazas (1 día)
- Impacto Potencial (1 día)
- Nivel de Riesgo (0,5 día)
- Nivel de riesgo aceptable (0,25 día)
- Nivel de riesgo residual (0,25 día)
- Categorización del sistema de acuerdo con el ENS (1 día)
- Nivel de calidad del dato aceptable (1 día)

TOTAL: 10 DÍAS

Fase 4.
Plazo para conseguirlo: del 7-11 al 26-11
Hitos a conseguir:
- Revisión de Fase 3 (1 día)
- Propuesta de Mejoras (4 días)
- Cuantificación económica y temporal (2 días)

TOTAL: 7 DÍAS

Fase 5.
Plazo para conseguirlo: del 27-11 al 11-12
Hitos a conseguir:
- Revisión de Fase 4 (1 día)
- Evaluación de los controles y la madurez (1 días)
- Evaluación del nivel de cumplimiento de las normativas y hallazgos (4 día)
- Presentación de resultados (1 día)

TOTAL: 7 DÍAS

Fase 6.
Plazo para conseguirlo: del 12-12 al 28-12
Hitos a conseguir:
- Revisión de Fase 5 (1 día)
- Video Resumen (1 día)
- Revisión de la memoria del trabajo de final de máster (1 día)
- Finalización de la memoria del trabajo de final de máster (1 días)
- Presentaciones PowerPoint (2 día)

TOTAL: 6 DÍAS

La unidad de tiempo es el día, cada día se corresponde con un total de aproximadamente 5 horas trabajadas. Se han establecido jornadas de trabajo de 5 horas para así poder dinamizar espacios de trabajo de mañana/tarde y no construir una planificación fija que no pueda afrontar imprevistos.

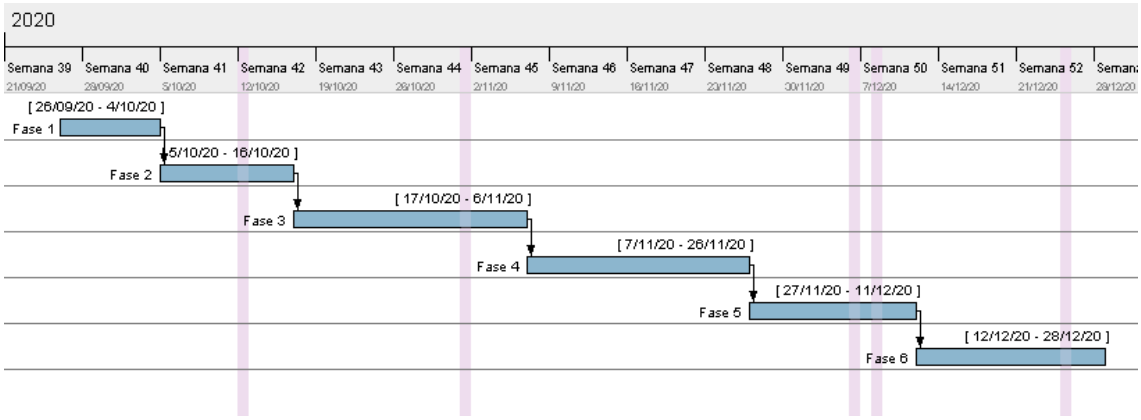

Figura 2 - Diagrama Gantt

El diagrama representa los intervalos de tiempo para cumplir con los hitos del trabajo, no representan el total de días necesarios para desarrollarlos.

1.5. Breve sumario de productos obtenidos

El presente trabajo de final de máster (TFM) ha generado los siguientes productos:

- ✔ Memoria de TFM (este documento: **memoria TFM.pdf**)
- ✔ Presentación con el resumen del proyecto. (**presentacion resumen TFM.odp**)
- ✔ Presentación con el resumen del análisis de riesgos. **(presentación AR.odp)**
- ✔ Video de presentación. **(video TFM.mp4)**
- ✔ Política de Seguridad.
- ✔ Decreto Comité de Seguridad.
- ✔ Plan de Adecuación al Esquema Nacional de Seguridad.
- ✔ Auditorias Internas.
- ✔ Declaración de Aplicabilidad.
- ✔ Plan de mejora de la seguridad.
- ✔ Análisis GAP del estado inicial de la organización para ISO/IEC 27001.
- ✔ Análisis GAP del estado inicial de la organización para ISO/IEC 27002.
- ✔ Ejemplo de Pliego de Prescripciones Técnicas para los proyectos propuestos.
- ✔ Análisis de riesgos: Dependencias entre Activos.
- ✔ Análisis de riesgos: Análisis de amenazas.
- ✔ Categorización del sistema.
- ✔ Software PILAR: plantilla ISO 27000:2013 para PILAR con gráficos radiales.
- ✔ Software PILAR: proyecto de análisis de riesgos.
- ✔ Software PILAR: proyecto de evaluación de madurez para ISO 27001.
- ✔ Software PILAR: proyecto de evaluación de madurez para ENS.

1.6. Breve descripción de los otros capítulos de la memoria

Capítulo 2: Contextualización, Objetivos y Análisis Diferencial. Estudiaremos el entorno de los sistemas de información a analizar, daremos importancia a los objetivos dentro de un marco organizativo y dibujaremos un punto de partida inicial en el cumplimiento de normativas.

Capítulo 3: Sistema de Gestión Documental. Estableceremos toda la base documental que apoyará nuestras labores de campo y nuestras conclusiones.

"Mens et manus" – Lema del MIT

Capítulo 4: Análisis de Riesgos. Conoceremos y valoraremos los riesgos asociados a los activos y en los que aplique calcularemos su aporte a la calidad del dato.

Capítulo 5: Propuesta de Proyectos. Se sugerirán proyectos que mejoren el estado de la seguridad de la organización y la calidad del dato y valoraremos sus costes asociados.

Capítulo 6: Auditoría de Cumplimiento. Comprobaremos el nivel de cumplimiento de la organización en el Esquema Nacional de Seguridad y la ISO/IEC 27002.

Capítulo 7: Conclusiones. Valoraremos el trabajo realizado y los aspectos negativos y positivos encontrados al añadir al Plan Director de Seguridad la visión de la Calidad del Dato.

2. Contextualización, objetivos y Análisis Diferencial

2.1. Contextualización

Para garantizar el anonimato de la entidad todos los datos se encuentran dentro de rangos de ofuscación. Para no emplear el nombre real se utilizará un pseudónimo. Además la información contenida en los documentos obtenidos en este TFM puede no corresponder con la situación real de la entidad.

Datos de la entidad:

Nombre: Ayuntamiento de la Universitat Oberta de Catalunya.
Tipo de ente: Administración Local.
Población: entre 18.000 y 25.000 habitantes.
Empleados Municipales: entre 140 y 200.
Empleados Municipales con acceso a sistemas de información: entre 80 y 100.
Presupuesto anual: entre 15 y 17 millones de euros.
Número total de sedes con acceso a datos: 18.

- Sedes gestionadas por el ayuntamiento: 9.
- Sedes de gestión mixta entre el Ayto y otra entidad: 4.
- Sedes gestionadas por la comunidad/diputación: 4.
- Sedes gestionadas por entidades privadas y otros organismos: 1.

Recursos Humanos del departamento TIC: Se dispone de un ingeniero técnico de sistemas y un FP de microinformática, además el concejal del área realiza algunas labores de mantenimiento tanto de hardware como de software.

2.1.1. Organigrama de la organización

Ver ANEXO I. Organigrama

Partimos de base con este organigrama, no obstante hay que destacar la existencia de una alta rotación y movilidad de trabajadores en esta administración.

El grueso del personal se encuentra en la Casa Consistorial, no obstante Urbanismo, Servicios Sociales y la Policía se encuentra en el edificio de Servicios Técnicos. La Policía además cuenta con una sede satélite. El departamento de cultura está distribuido entre el Centro Polivalente, el Auditorio Municipal y la Biblioteca. Finalmente Deportes se encuentra en el Polideportivo Municipal.

2.1.2. Infraestructura Física

Ver ANEXO II. Diagrama de Estructura Física

Vamos a realizar una descripción detallada de la Infraestructura centrándonos en los elementos críticos de la misma.

El Ayuntamiento de la UOC renovó sus sistemas virtualizando la mayoría de los escritorios, su CPD se encuentra en la Casa Consistorial y cuenta con la siguiente equipación principal:

- Información no disponible
- Información no disponible
- Información no disponible
- Información no disponible
- Información no disponible
- Información no disponible
- Información no disponible
- Información no disponible

Información no disponible

Información no disponible
Información no disponible

Información no disponible

Figura 3 - Diagrama simplificado estructura de red.

Información no disponible
Información no disponible

Información no disponible
Información no disponible
Información no disponible

Información no disponible
Información no disponible

Información no disponible

La puerta de entrada tanto al despacho de informática como al CPD, a la que se accede desde el propio despacho, se encuentra securizada con alarma en circuito independiente y validación y registro mediante tarjetas RFID.

2.1.3. Infraestructura Lógica

El Ayuntamiento cuenta con las siguientes máquinas en su entorno virtualizado de infraestructura:
Información no disponible
Información no disponible
Información no disponible
Información no disponible
Información no disponible
Además existen una serie de máquinas adicionales que se utilizan como entorno de pruebas.

En el entorno virtualizado de VDI encontramos las siguientes máquinas:
Información no disponible
Información no disponible

2.1.4. Principales Proveedores de Servicios

El Ayuntamiento cuenta con tres servidores cloud en modo IaaS para labores de correo electrónico y servicios web, el proveedor se encuentra certificado en ENS a nivel medio para el servicio contratado. El gestor de expedientes y la sede electrónica está gestionado por un proveedor externo en modo SaaS, el proveedor se encuentra certificado en ENI y en ENS a nivel alto para el servicio contratado. Se cuenta con un único ISP tanto para datos como telefonía (móvil y fija), el proveedor se encuentra certificado en ENS a nivel básico para los servicios contratados. Se cuenta con un proveedor que monitoriza 24/7 la infraestructura del CPD para mantenimiento correctivo, el proveedor se encuentra certificado en ISO/IEC 27001. Se cuenta con distintos servicios de soporte para las aplicaciones de nóminas, policía, padrón, recaudación, contabilidad, etc.

2.1.5. Entorno de Red

El Ayuntamiento cuenta en su CPD con varias VLANs para distintos aspectos como son la vlan de infraestructura, la de servicio, la de usuarios, la de Mancomunidad (organización que opera desde las instalaciones del Ayuntamiento, **ver ANEXO II. Diagrama de Estructura Física**) y otras de menor importancia.

La VLAN de usuarios es accesible desde
Información no disponible
Información no disponible

Información no disponible
Información no disponible
Información no disponible

El Ayuntamiento cuenta con dos VPNs activas, una para labores de monitorización y otra para conectividad con otras Administraciones Públicas (Red Sara).

2.2. Plan Director de Seguridad

Una vez conocida la infraestructura, se establecerán en primer lugar el alcance y los objetivos del Plan Director de Seguridad y posteriormente los de Calidad del Dato.

2.2.1. Alcance

Este plan se centra en los sistemas de información que dan soporte al modelo de negocio de la organización, la infraestructura a analizar abarcará el entorno tanto físico como lógico, su red, sus proveedores y el personal de la organización con acceso a datos. Excluiremos el servicio de telefonía tanto móvil como fija por motivos de adaptación al tiempo disponible para realizar este trabajo, esto incluye la centralita telefónica analógica. Excluiremos del alcance otros elementos menores de IOT que dispone el ayuntamiento, como luminarias, ascensores, aires acondicionados, videovigilancia, alarmas, etc., en el caso de que alguno de estos elementos se encuentre relacionado directamente con alguno de los sistemas de información objeto de estudio, se incluirá en el alcance. Excluiremos el sistema Wifi que aunque es un servicio para el ciudadano, por él no circulan datos de la organización.

Por otra parte las sedes elegidas para realizar el trabajo serán: Casa Consistorial, Servicios Técnicos, Centro Polivalente, Satélite Policía, Biblioteca y un entorno modelo de Teletrabajo. Siendo estas las sedes más relevantes en el acceso a sistemas de información.

2.2.2. Objetivos

Cumplir el Esquema Nacional de Seguridad, ISO/IEC 27001, el RGPD, la LOPDGDD y las buenas prácticas de ISO/IEC 27002, finalidad:

- Aumentar la confianza de los ciudadanos en el Ayuntamiento.
- Proteger las características de la información: disponibilidad, integridad y confidencialidad.
- Identificar y mitigar riesgos.

2.2.2.1. Esquema Nacional de Seguridad

El RD 3/2010 [43] regula el Esquema Nacional de Seguridad (modificado por El RD 951/2015 [1]) de obligado cumplimiento para las administraciones públicas como se definió que tenían que operar en las leyes 39/2015 del Procedimiento Administrativo Común [44] y 40/2015 de Régimen Jurídico del Sector Público [45], ambas en vigor y actualizadas este pasado Septiembre de 2020.

Son objetivos del ENS los nombrados en el artículo 4 del RD 3/2010 [1]:

- Seguridad como proceso integral: compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema de información.
- Gestión de riesgos: manteniéndose permanentemente actualizado.
- Prevención, Reacción y Recuperación: evitando la materialización de las amenazas que afecten al patrimonio digital del sistema de información.
- Líneas de defensa: estrategia de seguridad que permita minimizar impacto, reducir la probabilidad de compromiso de datos y ganar tiempo de reacción.
- Revaluación periódica: el sistema de información cambia, las amenazas cambian, por lo tanto, las medidas de seguridad se revalúan y se actualizan.
- Función diferenciada: **no** son lo mismo el responsable de información, el responsable de servicio y el responsable de seguridad, la política de seguridad tiene que detallar las atribuciones de cada uno.

El Centro Criptológico Nacional, CERT Gubernamental de España, se encarga de la elaboración de las guías CCN-STIC muy útiles en diversas disciplinas de seguridad y en concreto existe la serie CCN-STIC-800 centrada en el ENS, para el desarrollo del TFM emplearemos entre otras las guías CCN-STIC 806 [38] y CCN-STIC 815 [24].

2.2.2.2. RGPD y LOPDGDD

El Reglamento General de Protección de datos aprobado el 27 de Abril de 2016 y en vigor [11] proviene del reglamento UE 2016/679 y es de obligado cumplimiento por las administraciones públicas. Establece tres principios básicos: principio de responsabilidad por el que las organizaciones tendrán que demostrar que han aplicado las medidas en materia de tratamiento de datos tal y como establece la norma; principio de protección de datos por defecto y desde el diseño inicial de las organizaciones/productos/servicios/actividades; y principio de transparencia con el empleo de políticas de privacidad simples e inteligibles [12].

Por lo tanto el RGPD establece nuevas obligaciones para la implantación de un SGSI en una organización europea:

- ART. 4. Listado de datos “sensibles” que requieren especial protección.
- ART. 32 Seguridad del tratamiento.
- ART. 33.1 Las violaciones de seguridad de los datos serán comunicadas a las autoridades de control en menos de 72 horas desde el incidente.

- ART. 35. Se convierten en obligatorias las evaluaciones de impacto relativas a la protección de datos, en particular si se utilizan nuevas tecnologías.
- ART. 37 y 38. Aparece una nueva figura, el Delegado de Protección de Datos, esta figura será distinta al responsable de seguridad o al responsable de servicio/información y tendrá un perfil jurídico, la normativa permite compartir DPD entre organismos, un punto a tener en cuenta en administraciones locales pequeñas/medianas.
- SIN ARTÍCULO. En todo el reglamento de hace referencia a las garantías adicionales necesarias para poder realizar transferencias internacionales de datos. Para nuestro trabajo será recomendable tener en cuenta que los datos de nuestra organización se encuentren físicamente en territorio europeo.

Por otro lado, la ley orgánica 3/2018 del 5 de diciembre de protección de datos personales y garantía de los derechos digitales (LOPDGDD), es la actualización nacional para dar equivalencia a la antigua LOPD (15/1999) con el RGPD y conseguir alineamiento europeo. Según la nueva LOPDGDD [14]:

"Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad."

El CCN ha desarrollado la herramienta PILAR que incluye un módulo para facilitar el cumplimiento del RGPD y será la que usemos en este trabajo [13], así mismo se emplearán también algunos conocimientos de la guía aún no publicada a fecha de entrega de este trabajo, CCN-STIC 881 [40] Impacto del RGPD en el ENS [15].

2.2.2.3. ISO/IEC 27001 – ISO/IEC 27002

ISO/IEC 27001, con origen en BS 7799 parte 1 e ISO/IEC 17799 es el estándar internacional ampliamente aceptado de seguridad de la información, publicado en 2005 por la International Organization for Standardization.

Son objetivos de ISO/IEC 27001 los nombrados en su capítulo 1 "Scope": desarrollar, implantar, mantener y actualizar un SGSI, para conseguirlo se basa en el ciclo deming o PDCA (Plan-Do-Check-Act).

ISO/IEC 27002 es el estándar de la familia ISO / IEC 27000 que cuenta con el código de buenas prácticas para la implantación de un SGSI y es el estándar que seguiremos para evaluar los controles en los distintos dominios de seguridad.

2.2.2.3.1. Compatibilidad entre ISO/IEC 27001 y ENS

Como indica la pregunta 12.1 del apartado de FAQs del CCN sobre el ENS [2]:

" […] *Si bien cabe señalar que aquellas organizaciones que se encuentren certificadas contra ISO 27001 tienen una buena parte del camino recorrido para lograr su conformidad con el ENS, toda vez que las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional.*[...]"

"[…] *el Esquema Nacional de Seguridad y la norma UNE ISO/IEC 27001:2013 difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen.*[...]*"*

Por lo anteriormente citado, este TFM no persigue la certificación inmediata en ISO/IEC 27001, que no es de obligado cumplimiento, prioriza la certificación ENS y persigue la aplicación de las buenas prácticas de ISO/IEC 27001 e ISO/IEC 27002 para en un futuro certificarse en esta norma también.

2.2.2.3.2. ISO/IEC 27701. Compatibilidad ISO/IEC 27001 y RGPD

ISO/IEC 27701 es la norma encargada de compatibilizar ISO/IEC 27001 y el RGPD tal y como se indica en su capítulo 1 "Scope" [16], extendiendo los estándares ISO/IEC 27001 e ISO/27002 con el fin de dotarlos de gestión de la privacidad dentro del contexto de la organización. Por motivos de falta de tiempo queda fuera de este TFM el análisis de este estándar, aunque en una aplicación real y con el fin de aunar esfuerzos y ahorrar costes sería necesario su estudio.

2.3. Plan de Evaluación de la Calidad del Dato

A continuación vamos a establecer el alcance y los objetivos del plan de evaluación de la calidad del dato que será un subconjunto del alcance del Plan Director de Seguridad, no es útil analizar Calidad del Dato en sistemas que queden fuera del anterior plan.

2.3.1. Alcance

Este plan se centra en los datos contenidos en los sistemas objeto de estudio del Plan Director de Seguridad y más en concreto en el contenido de: software de padrón, el

gestor de expedientes actual, herramienta de policía, carpetas compartidas, active directory, correo electrónico, programa de nóminas, base de datos del software de fichaje y software de contabilidad y recaudación.

Queda excluido del estudio datos pertenecientes a sistemas de información donde ya no se realiza actualización de datos como puede ser el gestor de expedientes antiguo, la contabilidad antigua, documentos físicos en papel[1], etc. información que se conserva por motivos legales.

2.3.2. Objetivos

Cumplir el esquema nacional de interoperabilidad y las buenas prácticas de ISO/IEC 25012, finalidad:

- Poner al ciudadano en el centro de la información de la Administración Pública.
- Acercar posturas entre seguridad y nuevas tecnologías basadas en la calidad del dato y por lo tanto entre la dirección y el área TIC.
- Ahorrar costes, la información es la nueva moneda en la era digital, cualquier mecanismo que aumente su calidad se traducirá en un ahorro económico [10].

2.3.2.1. Esquema Nacional de Interoperabilidad

El RD 4/2010 [3] regula el Esquema Nacional de Interoperabilidad de obligado cumplimiento para las administraciones públicas y, como sucedía con el ENS, basado en las leyes 39/2015 [44] y 40/2015 [45].

Son objetivos del ENI los nombrados en el artículo 4 del RD 4/2010 [3]:

- Interoperabilidad como cualidad integral: de los sistemas de información en su ciclo de vida completo.
- Carácter multidimensional de la interoperabilidad: contemplando sus dimensiones organizativa, semántica, técnica y temporal.
- Enfoque de soluciones multilaterales: aproximación multilateral, modular y multiplataforma donde primará el compartir, reutilizar, y colaborar.

Si bien las guías CCN-STIC-800 no abarcan directamente el ENI, sí que se han escrito de modo que sean compatibles entre sí por lo que adecuar una administración al ENS implica dar pasos hacia el ENI, no obstante se cuenta con una guía de aplicación desde el área de descargas del portal de administración electrónica [4] que servirá de referencia.

1 *Aunque ISO/IEC 25012 no contemple el documento en papel, ENS y ENI sí que lo abordarán en aspectos de seguridad e interoperabilidad.*

2.3.2.2. ISO/IEC 25012 – ISO/IEC 25024 – ISO/IEC 25040

ISO/IEC 25012 es el estándar de la serie ISO/IEC 25000 SquaRE (System and Software Quality Requirements and Evaluation) dedicada al Modelo de la Calidad de Datos. Esta serie tiene su origen en los estándares ISO/IEC 9126 y ISO/IEC 14598.

Son objetivos de ISO/IEC 25012 los nombrados en su capítulo 1 “Scope”: definición de modelo de calidad de datos contenidos en un sistema de información y definición de las características de la calidad del dato en los sistemas de información permitiendo definir métricas de calidad, establecer criterios de calidad y evaluar la calidad de los datos.

ISO/IEC 25024 es el estándar que define métricas con las que cuantificar las características de la calidad de datos establecida en ISO/IEC 25012 y será empleada para evalular estas características.

ISO/IEC 25040 es el estándar que define la metodología para evaluar un producto software en cinco fases: Establecer los requisitos de evaluación, definir la evaluación, diseñar la evaluación, ejecutar la evaluación y concluir la evaluación. Será nuestra guía a la hora de diseñar el Plan de Modelado de Calidad del Dato.

Para trabajar la calidad del dato nos basaremos en el trabajo de (Verdugo y Rodríguez, 2020) [5] de un modo simplificado y que se detallará en la Fase 3 del TFM.

El objetivo de la evaluación de la calidad de los datos de este trabajo no reside en la exactitud de las métricas, que pueden tratarse de meras aproximaciones, si no de su posterior influencia en las propuestas de mejora de la fase 4 y en como estas afectan a las conclusiones obtenidas durante el análisis de riesgos y en la adaptación al ENS.

2.4. Análisis Diferencial

Este análisis se realiza a alto nivel y pretende contextualizar el grado de seguridad inicial de la organización de manera global con el fin de conocer el punto de partida.

2.4.1. Esquema Nacional de Seguridad

Para el análisis diferencial del ENS vamos a emplear la herramienta CLARA [6] desarrollada por el CCN sobre tres equipos estratégicos todos con sistemas Windows: el servidor de padrón, un escritorio de usuario VDI y un servidor cloud sin información confidencial. Esta herramienta se basa en las Guías CCN-STIC 850A, 850B, 851B, 870A, 870B, 570A, 570B, 599A18, 599B18, 599A19 y 599B19. Conforme avancemos en nuestro TFM categorizaremos nuestro sistema en BAJO, MEDIO o ALTO, puesto que aún desconocemos cual será el resultado de esta categorización vamos a utilizar

para este análisis los tres equipos de modo que cada uno se corresponda con una de las categorías atendiendo a su criticidad.

Servidor de Padrón:
Categorización del sistema según ENS: ALTO. Un incidente de seguridad supone un perjuicio muy grave.
Resultado:
Control ENS – Cumplimiento del Control
OP.ACC.4 - Proceso de gestión de derechos de acceso (80%)
OP.ACC.5 - Mecanismos de autenticación (51,25%)
OP.ACC.6 - Acceso local (60,86%)
OP.EXP.2 - Configuración de seguridad (62,28%)
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 (88,89%)
OP.EXP.10 - Protección de los registros de actividad (75%)
MP.EQ.2 - Bloqueo de puesto de trabajo (70%)
MP.EQ.3 - Protección de equipos informáticos (100%)
MP.COM.3 - Protección de la autenticidad y de la integridad (53,33%)

Servidor Cloud sin información confidencial:
Categorización del sistema según ENS: MEDIO. Un incidente de seguridad supone un perjuicio grave.
Resultado:
Control ENS – Cumplimiento del Control
OP.ACC.4 - Proceso de gestión de derechos de acceso (80%)
OP.ACC.5 - Mecanismos de autenticación (51,25%)
OP.ACC.6 - Acceso local (60,86%)
OP.EXP.2 - Configuración de seguridad (62,28%)
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 (100%)
OP.EXP.10 - Protección de los registros de actividad (100%)
MP.EQ.2 - Bloqueo de puesto de trabajo (70%)
MP.EQ.3 - Protección de equipos informáticos (100%)
MP.COM.3 - Protección de la autenticidad y de la integridad (66,67%)

Escritorio de Usuario VDI:
Categorización del sistema según ENS: BAJO. Un incidente de seguridad supone un perjuicio limitado.
Resultado:
Control ENS – Cumplimiento del Control
OP.ACC.4 - Proceso de gestión de derechos de acceso (80%)
OP.ACC.5 - Mecanismos de autenticación (100%)
OP.ACC.6 - Acceso local (86,67%)
OP.EXP.2 - Configuración de seguridad (32,28%)
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 (100%)
MP.EQ.2 - Bloqueo de puesto de trabajo (100%)
MP.COM.3 - Protección de la autenticidad y de la integridad (70%)

2.4.2. ISO/IEC 27001

Este análisis se lleva a cabo mediante el empleo de la herramienta GAP ISO/IEC 27001 de ISO27001security [17] y que se agrega como **producto obtenido del TFM (Gap_Inicial_ISO27001_2020.xml)**. La metodología empleada para la evaluación de los controles es la definida por COBIT y basada en CMM (Capability Maturity Model) de la Carnegie Mellon School. Para la evaluación de cada control se ha empleado la guía web de normaiso27001 [8].

Resultado obtenido:

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0 %	100 %
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	67 %	0 %
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	33 %	0 %
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0 %	0 %
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	0 %	0 %
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0 %	0 %
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0 %	0 %
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0 %	0 %
	Total	100 %	100 %

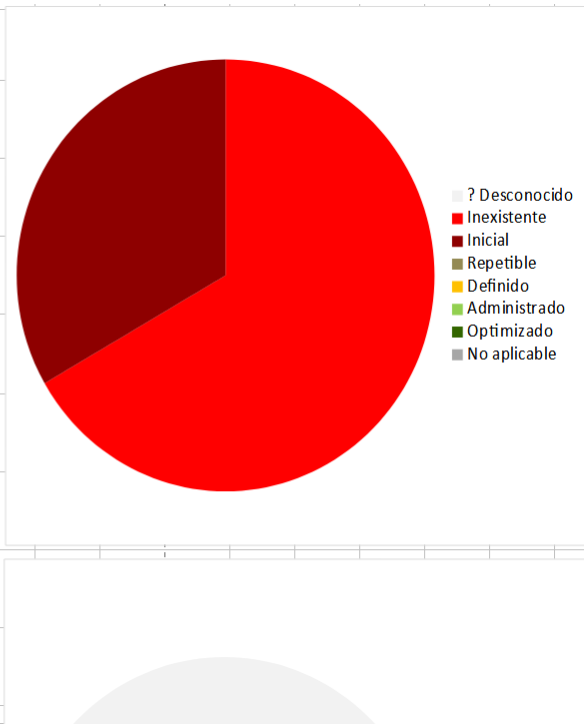

Figura 4 - Valores y Gráfico Inicial ISO/IEC 27001

2.4.3. ISO/IEC 27002

Este análisis se lleva a cabo mediante el empleo de la herramienta GAP del Wiki de SGSI del campus de la UOC [7] y que se agrega como **producto obtenido del TFM (Gap_Inicial_ISO27002_2020.xml).** La metodología empleada para la evaluación de los controles es la definida por COBIT y basada en CMM (Capability Maturity Model) de la Carnegie Mellon School. Para la evaluación de cada control se ha empleado la guía web de normaiso27001 [8].

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

Figura 5 - Metodología Empleada Análisis GAP

Resultado obtenido:

	r
A.5 Information security policies	1,5
A.6 Organization of information security	1
A.7 Human resource security	1,889
A.8 Asset management	1
A.9 Access control	2,25
A.10 Cryptography	1
A.11 Physical and environmental security	1,694
A.12 Operations security	1,929
A.13 Communications security	2,292
A.14 System acquisition, development and maintenance	2,014
A.15 Supplier relationships	2,833
A.16 Information security incident management	1,286
A.17 Information security aspects of business continuity management	2,333
A.18 Compliance	0,867

Figura 6 - Valores iniciales de ISO/IEC 27002

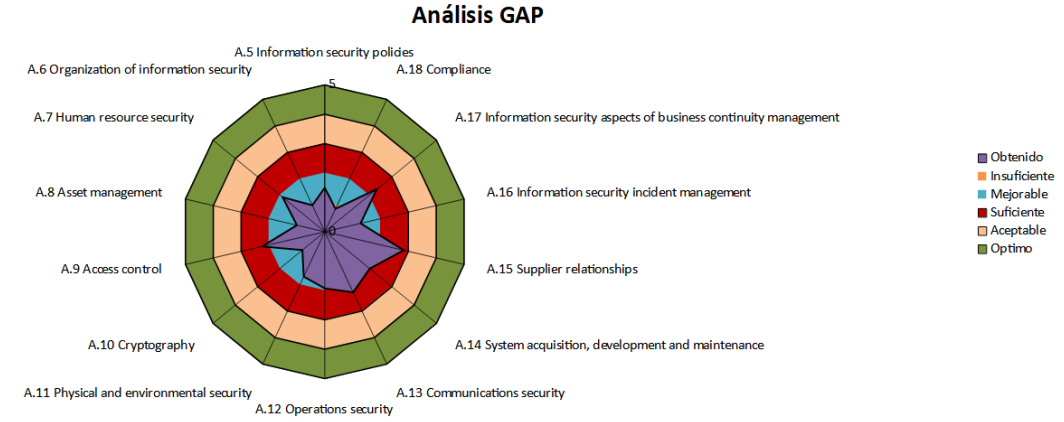

Figura 7 - Gráfico Radial inicial ISO 27002

2.4.4. Esquema Nacional de Interoperatibilidad

Para el análisis de adecuación inicial al ENI vamos a emplear la guía del PAe [4] de adecuación al ENI para cada uno de sus objetivos. **Ver ANEXO III. Análisis Diferencial ENI** Resultados:

- Interoperabilidad organizativa: Cumplimiento Medio
- Interoperabilidad semántica: Cumplimiento Medio
- Interoperabilidad técnica: Cumplimiento Medio-Alto
- Infraestructuras y servicios comunes: Cumplimiento Alto
- Comunicaciones de las Administraciones Públicas: Cumplimiento Alto
- Reutilización y transferencia de tecnología: NO APLICA
- Firma electrónica y certificados: Cumplimiento alto
- Recuperación y conservación del Doc. Electrónico: Cumplimiento insuf.
- Normas de conformidad: Cumplimiento insuficiente

3. Sistema de Gestión Documental

3.1. Plan de Adecuación al Esquema Nacional de Seguridad

Para desarrollarlo se emplea la Guía de Seguridad de las TIC CCN-STIC 883 para Ayuntamientos menores de 20.000 habitantes [18]. Esta decisión se toma por el presupuesto limitado del que dispone el Ayuntamiento de la UOC y su modo de organización, además de que su población se encuentra cercana a esta cifra.

Ver producto obtenido del TFM (Plan de Adecuación al ENS.pdf)

El Plan de Adecuación es el punto final para el cumplimiento del Esquema Nacional de Seguridad. En él se incluye toda la documentación que se ha desarrollado para el cumplimiento con el ENS, en concreto: Política de Seguridad, Categorización del Sistema, Análisis de Riesgos, Declaración de Aplicabilidad y Plan de Mejora de la Seguridad. Para el desarrollo de toda esta documentación, además de las guías específicas nombradas en cada apartado, se utilizan las guías generales para el ENS CCN-STIC 803 [35], CCN-STIC 804 [36], CCN-STIC 805 [37], CCN-STIC 806 [38], CCN-STIC 808 [39] y CCN-STIC 815 [24].

Este documento es específico del ENS. El resultado final tiene que incluir todos los documentos anteriormente citados, en nuestro caso y por claridad con respecto a otros estándares como ISO/IEC 27001:2013 los presentaremos de forma separada.

3.2. Política de Seguridad.

Para desarrollarla se emplea como base la Guía de Seguridad de las TIC CCN-STIC 883 para Ayuntamientos menores de 20.000 habitantes [18].

Ver producto obtenido del TFM (Política de Seguridad.pdf)

La Política de Seguridad definirá el propósito general de nuestro SGSI y cómo conseguirlo, si bien puede incidir en algunos temas específicos en su mayoría tendrá un corte generalista. Este documento tiene que ser aprobado por la dirección y revisado periódicamente, es obligatorio tanto para el ENS como para ISO/IEC 27001:2013.

3.2.1. Adaptación a ISO/IEC 27001

Nuestra política de seguridad tiene aproximaciones a ISO/IEC 27001:2013. Vamos a enunciar por una parte las características de la Política de Seguridad en la norma y por otra lo redactado en nuestra política de seguridad del ENS:

- Apartado 5.1.a) de la norma "[…] asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización [...]", se establece en el apartado 3. "Misión del Ayuntamiento de la UOC".
- Apartado 5.2.a) de la norma "[…] sea adecuada al propósito de la organización […]", se establece en el apartado 3. "Misión del Ayuntamiento de la UOC".
- Apartado 5.2.b) de la norma "[…] incluya objetivos de seguridad de la información […]" se establece en el apartado 2. "Introducción", enumerando las características básicas de la información: disponibilidad, integridad y confidencialidad.
- Apartado 5.2.c) de la norma "[…] incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información […]". se establece en el apartado 7.4. "Funciones del comité de seguridad de la información.
- Apartado 5.2.d) de la norma "[…] incluya el compromiso de mejora continua del SGSI […]" se establece en el apartado 7.4. "Funciones del comité de seguridad de la información".
- Compromiso de la gerencia: ISO/IEC 27001:2013 propone que la política de seguridad debe tener aprobación explícita por parte de la dirección, esta se añade al final del capítulo 2. "Introducción".
- Se define el marco jurídico y normativo del SGSI en el capítulo 4. "Marco normativo".

Además se realizan modificaciones en el documento para agregar referencias al estándar ISO/IEC 27001:2013 e ISO/IEC 27002:2013 donde corresponda y se redefinen algunos puntos para que no sean referencia exclusiva al ENS.

Otros recursos empleados en la elaboración de la Política de Seguridad del SGSI: [19] y [20].

3.2.2. Casuística local del Ayuntamiento de la UOC

En el marco normativo se ha presupuesto que el Ayuntamiento de la UOC se encuentra en la Comunidad Autónoma de Cataluña.

3.2.3. Aprobación del Comité de Seguridad.

Al igual que sucede con ISO/IEC 27001:2013, una vez elaborada la política de seguridad, el comité de seguridad tiene que ser respaldado por la dirección del organismo, en el caso de la Administración Local una forma de aprobarlo es mediante

decreto de Alcaldía, se propone un decreto como ejemplo obtenido de la guía CCN-STIC 883 [18], de este modo la constitución del comité de seguridad queda publicada oficialmente tanto en el tablón físico de anuncios como en la Sede Electrónica.

Ver producto obtenido del TFM (Decreto Comité de Seguridad.pdf) Incluye la propuesta a la alcaldía y el propio decreto.

De este modo el Comité de Seguridad se convierte en un órgano colegiado del Ayuntamiento, al mismo nivel que la Junta de Gobierno Local ó el Pleno. Se trata de un paso previo a la aprobación de la Política de Seguridad.

3.3. Procedimiento de Auditorías Internas.

Para desarrollarlo se emplea la Guía de Seguridad de las TIC CCN-STIC 802 Guía de auditoría [21].

Ver producto obtenido del TFM (Procedimiento de Auditorías Internas.pdf)

Otras fuentes empleadas [22] [17] [23].

3.4. Gestión de Indicadores

Se emplea para su desarrollo las indicaciones de la Guía CCN-STIC 815 Métricas e Indicadores [24].

3.4.1. Indicadores de madurez

Los niveles de madurez serán los siguientes:

- L0 – Inexistente. En el nivel L0 de madurez no hay nada.
- L1 - Inicial / ad hoc. En el nivel L1 de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de la alta calidad.
- L2 - Reproducible pero intuitivo. En el nivel L2 de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
- L3 - Proceso definido. Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

- L4 – Gestionado y medible. Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
- L5 – Optimizado. El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

3.4.2. Indicadores Anexo II Esquema Nacional de Seguridad

El ENS establece una serie de medidas de protección en su Anexo II. Se establece un nivel de madurez de referencia para cada medida de protección atendiendo a la categoría del sistema:

- BAJA. Requiere un indicador de madurez al menos L2, reproducible pero intuitivo.
- MEDIA. Requiere un indicador de madurez al menos L3, proceso definido.
- ALTA. Requiere un indicador de madurez al menos L4, gestionado y medible.

3.5. Procedimiento de Revisión por Dirección

Aunque esta reunión sólo se plantea para el cumplimiento de la norma ISO/IEC 27001:2013 es recomendable unificarla con otras reuniones para otras normas como por ejemplo el RGPD, la evaluación de Calidad del Dato o incluso la norma ISO/IEC 9001.

3.5.1. Asistentes

Se eligen los siguientes cargos y responsabilidades:

- Alcalde-Presidente.
- Concejal de Nuevas Tecnologías (Informática y Deportes).
- Concejal de Economía y Hacienda.
- Concejal de Seguridad y Obras.
- Concejal de Personal.
- Responsable de Seguridad.

Se opta por un modelo que atiende a la casuística local del Ayuntamiento de la Universitat Oberta de Catalunya. Los seleccionados son cargos que se encuentran liberados al 100% o que tienen alta dedicación al Ayuntamiento, también por estas condiciones son los que mayor peso tienen en la toma de decisiones.

El concejal de Personal puede representar al resto de concejalías no presentes dado que mantiene estrecho contacto con todos los responsables departamentales del Ayuntamiento.

Con el fin de agilizar la reunión el responsable de seguridad facilitará en la convocatoria de la reunión a los concejales, a través de sede electrónica, toda la información relevante a los puntos a tratar. Se aconseja que los concejales elaboren un microinforme previo del estado de la seguridad de la información de sus respectivas áreas [26].

El responsable de seguridad será el encargado de dirigir la reunión y actuar de secretario de la misma para documentarla adecuadamente. También será el responsable del custodio de la documentación resultante de las revisiones de la dirección.

3.5.2. Frecuencia

Se realizará de forma ordinaria al menos una vez al año y al menos con un mes de antelación sobre la siguiente auditoría interna a realizar. Será posible adelantar la fecha la reunión si el informe de la anterior auditoría ya se encuentra disponible.

3.5.3. Objetivos

Son objetivos de esta reunión la evaluación de los resultados de la gestión de la seguridad de la información con el fin de alinear e implicar a la dirección y tomar las decisiones estratégicas para garantizar que los objetivos del SGSI sigan siendo los adecuados.

Es objetivo también revisar la validez de los problemas identificados y los riesgos de organización [25].

3.5.4. Puntos a tratar

Basados en el punto 9.3 de ISO/IEC 27001:2013:

- Estado de las acciones de revisiones de gestión anteriores.
- Cambios en problemas externos e internos que son relevantes para el sistema de gestión de la seguridad de la información. En este punto se puede decidir si estos cambios afectan sustancialmente a la Política de Seguridad del Ayuntamiento.
- Retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:
  - No conformidades y acciones correctivas.
  - Resultados de monitoreo y medición.
  - Resultados de auditoría.
  - Cumplimiento de los objetivos de seguridad de la información.

- Retroalimentación de las partes interesadas. Es en este punto donde los concejales de las respectivas áreas pueden aportar su visión y exponer su microinforme.
- Análisis del los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.
- Evaluar las oportunidades para la mejora continua.
- Planificación de fechas y esquema de la próxima auditoría.

Si se dispone del informe de auditoría del ENS, además de añadir los resultados a los anteriores puntos, se puede añadir un punto de revisión del Plan de Adecuación al Esquema Nacional de Seguridad.

ISO/IEC 27001:2013 señala que de esta reunión se obtendrán decisiones en firme por parte de la dirección en materias como mejora continua o necesidades de cambio estratégicas sobre el SGSI.

3.6. Gestión de Roles y Responsabilidades

Se emplearán como base los roles del Esquema Nacional de Seguridad aplicados al tamaño del Ayuntamiento de la Universitat Oberta de Catalunya, aunque realizaremos también una equivalencia con los roles necesarios para el desarrollo de un Plan Director de Seguridad y el RGPD.

3.6.1. Roles ENS

Los roles son los enumerados en la guía CCN-STIC 801 [30].

Como se expone en la Política de Seguridad del Ayuntamiento, disponemos de los siguientes roles:

- Responsable de Información: SECRETARIO.
- Responsable de los Servicios: SECRETARIO.
- Responsable de Seguridad: TÉCNICO DE URBANISMO.
- Responsable del Sistema: TÉCNICO DE INFORMÁTICA.
- Comité de Seguridad.

Los miembros y funciones del Comité de Seguridad, así como las funciones de los distintos roles se exponen en el apartado 7 “Organización de la Seguridad”, de la Política de Seguridad del Ayuntamiento.

Como responsable de seguridad se ha asignado a un técnico de Urbanismo, esto es debido en primer lugar a que el responsable de seguridad y el de sistemas no pueden coincidir en la misma persona, el técnico de urbanismo es ingeniero informático y además tiene conocimientos de seguridad de la información.

Al tratarse de un Ayuntamiento pequeño-mediano, por recursos disponibles, se decide que el responsable de información y el de servicio recaiga sobre la misma persona.

El Secretario del Comité de Seguridad es el Técnico Jurídico de RRHH, de este modo se garantiza que dentro de los planes de formación se incluya lo relativo a la Seguridad de la Información, dando así un peso importante al aspecto de la seguridad donde el eslabón más débil suele ser el propio personal municipal.

3.6.2. Roles Plan Director de Seguridad

Director ejecutivo (Chief Executive Officer, CEO), es el responsable último del Ayuntamiento, se corresponde con el Alcalde-Presidente.

Director de Tecnologías de la Información (Chief Information Officer, CIO), es el responsable de la tecnología de la información del Ayuntamiento, se corresponde con las funciones del rol ENS Responsable del Sistema.

Director de Sistemas (Chief Tecnology Officer, CTO), es el responsable de la gestión de las tecnologías de la información, al tratarse de una entidad pequeña este rol será cubierto igualmente por el rol ENS Responsable del Sistema.

Director de Seguridad de la Información (Chief Information Security Officer, CISO), es el responsable de garantizar la seguridad de la información del Ayuntamiento, se corresponde con las funciones del rol ENS Responsable de Seguridad.

Responsable de seguridad de la organización (Chief Security Officer, CSO), es el responsable de la seguridad física y tecnológica del Ayuntamiento, al tratarse de una entidad pequeña este rol será cubierto igualmente por el rol ENS Responsable de Seguridad.

3.6.3. Roles RGPD UE 2016/679 y LOPDGDD

Responsable del tratamiento. Según RGPD art. 4.7 y LOPDGDD Título V es *"La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.*". El propio Ayuntamiento de la Universitat Oberta de Catalunya es el Responsable del Tratamiento (persona jurídica).

Encargado del tratamiento. Según RGPD art. 4.8 y LOPDGDD Título V es "*La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento.*". El propio Ayuntamiento de la Universitat Oberta de Catalunya es el Encargado del Tratamiento (persona jurídica).

Delegado de Protección de Datos. RGPD, art.39 y LOPDGDD arts. 34 a 37, donde se indica que el DPD tendrá funciones de información, asesoramiento y supervisión de la normativa del RGPD. En el Ayuntamiento de la UOC el DPD recae sobre una empresa externa al no disponer de personal especializado en el campo y no tener recursos para contratar uno de dedicación exclusiva. En concreto el DPD se comparte con otras tres entidades locales cercanas (dos municipios y una mancomunidad).

3.7. Metodología de Análisis de Riesgos

El Ayuntamiento de la Universitat Oberta de Catalunya ha realizado un análisis de riesgos, según lo establecido en el Anexo II del Real Decreto en su sección [op.pl.1], conforme a lo establecido en el Perfil de Cumplimiento Específico de aplicación a Ayuntamientos de menos de 20.000 habitantes.

El análisis de riesgos ha sido realizado usando la metodología MAGERIT en su versión 3.0. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

MAGERIT es adecuada tanto para el análisis de riesgos en base al Esquema Nacional de Seguridad, al Reglamento General de Protección de Datos (RGPD) y al estándar internacional ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

3.7.1. Herramienta para el Análisis de Riesgos

Según la Guía CCN-STIC 882 Guía de Análisis de Riesgos para Entidades Locales [31], se recomienda el empleo de la herramienta PILAR del CCN, en nuestro caso emplearemos tanto la versión que incluye el perfil del ENS como la versión con el perfil ISO/IEC 27000.

PILAR implementa la metodología MAGERIT versión 3.0 y es la que emplearemos como herramienta de apoyo en el análisis de riesgos del Ayuntamiento de la Universitat Oberta de Catalunya.

3.7.2. Identificación y valoración de activos

Identificación y valoración de activos obtenida de el Libro II de Magerit (Catálogo de Elementos, capítulos 2, 3, y 4) [27]:

- Activos esenciales: son aquellos que representan las actividades principales que ofrece el Ayuntamiento a los ciudadanos. Incluyen tanto información como servicios. Los datos de carácter personal forman parte de ellos. Marcan los requisitos de seguridad para todos los demás componentes del sistema.

- [D] Datos/Información: activos abstractos (no físico), normalmente se presenta en forma de ficheros o bases de datos y es almacenado en equipos o soportes de información.
- [S] Servicios: activos que representan a servicios prestados por el sistema de información del Ayuntamiento como el email, el ftp, el servicio de directorios, etc.
- [SW] Software: activos en forma de aplicaciones informáticas.
- [HW] Hardware: equipamiento físico informático.
- [COM] Redes de comunicaciones: contando tanto servicios internos como contratados a terceros.
- [AUX] Equipamiento auxiliar: activos que dan apoyo a otros activos del sistema de información como pueden ser UPS, cableado, armarios, etc.
- [L] Instalaciones: lugares que alojan activos de los sistemas de información.
- [P] Personal: personas que utilizan los sistemas de información del Ayuntamiento, incluidos proveedores.

Todos los activos anteriores serán valorados atendiendo a las características que dan valor a un activo, que son:

- [D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. (UNE 71504:2008).
- [I] Integridad de los datos: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada (ISO/IEC 13335-1:2004).
- [C] Confidencialidad de la información: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados (UNE-ISO/IEC 27001:2007).
- [A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos (UNE 71504:2008).
- [T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad (UNE 71504:2008).

Todos los activos serán valorados atendiendo a las anteriores características empleando estos criterios de valoración:

- Extremo (10): Daño extremadamente grave.
- Muy alto (9): Daño muy grave.
- Alto (6-8): Daño grave.
- Medio (3-5): Daño importante.
- Bajo (1-2): Daño menor.
- Despreciable (0): Irrelevante a efectos prácticos.

3.7.3. Identificación y valoración de amenazas y vulnerabilidades

Identificación y valoración de amenazas y vulnerabilidades obtenida de el Libro II de Magerit (Catálogo de Elementos, capítulo 5) [27]:

- [N] Desastres naturales: de origen natural accidental, incluye daños por fuego [N.1], por agua [N.2] y desastres naturales [N.*].
- [I] De origen industrial: de origen industrial accidental derivados de la actividad humana, incluye daños por fuego [I.1], daños por agua [I.2], daños por contaminación mecánica [I.3], daños por contaminación electromecánica [I.4], averías de origen físico o lógico [I.5], desastres industriales [N.*], etc.
- [E] Errores y fallos no intencionados: de origen accidental derivados de la actividad humana, incluye errores de los usuarios [E.1], errores de los administradores [E.2], errores de monitorización [E.3], errores de configuración, [E.4], escapes de información [E.14], etc.
- [A] Ataques intencionados: de origen deliberado derivado de la actividad humana, incluye manipulación de los logs [A.3], manipulación de la configuración [A.4], suplantación de la identidad del usuario [A.5], etc.

Las anteriores amenazas se valorarán de acuerdo a la probabilidad de que se materialicen empleando los siguientes niveles: VR muy extraño, U improbable, P posible, VH probable y AC prácticamente segura.

3.8. Declaración de Aplicabilidad

Para desarrollarla se emplea como base la Guía de Seguridad de las TIC CCN-STIC 883 para Ayuntamientos menores de 20.000 habitantes [18] y la CCN-STIC-852 [32].

Ver producto obtenido del TFM (Declaración de Aplicabilidad.pdf)

La declaración de aplicabilidad incluida de ISO 27001:2013 se adapta para coincidir con la declaración de aplicabilidad del ENS por lo tanto puede no ser válida para una certificación ISO donde tendremos que revaluarla atendiendo a los objetivos del estándar.

Otras fuentes empleadas: [17] [28].

3.9. Plan de Mejora de la Seguridad

Para desarrollarla se emplea como base la Guía de Seguridad de las TIC CCN-STIC 883 para Ayuntamientos menores de 20.000 habitantes [18] y la CCN-STIC-852 [32].

Ver producto obtenido del TFM (Plan de mejora de la Seguridad.pdf)

3.10. Plan de Modelado de Calidad del dato

Este plan supondrá una versión muy simplificada de la elaborada por Verdugo y Rodríguez [5], además seguiremos la guía de Calabrese y Esponda [34].

3.10.1. Establecer los requisitos de evaluación

El propósito de la evaluación es determinar si la información contenida en los datos del Ayuntamiento de la Universitat Oberta de Catalunya cumple con los formatos esperados, cómo de eficazmente puede recuperarse y qué grado de ciberseguridad dispone.

Para calcular este propósito seleccionaremos las características de:

- Confidencialidad: para saber que los datos sólo son accedidos por usuarios autorizados.
- Trazabilidad: se analiza si los datos proporcionan un registro de modificaciones.
- Disponibilidad: es el grado en que los datos pueden ser obtenidos por los usuarios.
- Conformidad: para evaluar que los datos cumplen con los estándares y las normativas vigentes.
- Recuperabilidad: donde se comprueba si los datos son tolerantes a fallos.

Todos los datos analizados serán dependientes del sistema, se excluye la calidad del dato inherente por no ser el objetivo de este TFM.

3.10.2. Especificar la Evaluación

A continuación vamos a definir los criterios de decisión para cada característica seleccionada para el propósito de evaluación:

Recuperabilidad (Tiempo medio de recuperación)	Inaceptable	Recuperable en más de 8 horas o no recuperable
	Mínimamente Aceptable	Recuperable en menos de 8 horas
	Rango Objetivo	Recuperable en menos de 2 horas
	Excede los Requerimientos	Recuperable en menos de 15 minutos
Conformidad	Inaceptable	No puede cumplir RGPD, ENS ni ENI a corto plazo
	Mínimamente Aceptable	Puede cumplir RGPD, ENS y ENI a corto plazo
	Rango Objetivo	Cumple RGPD, ENS y ENI

	Excede los Requerimientos	Cumple RGPD, ENS, ENI y otros
Trazabilidad	Inaceptable	No existe trazabilidad
	Mínimamente Aceptable	Existe trazabilidad de acceso de usuarios con histórico de al menos un mes
	Rango Objetivo	Existe trazabilidad de acceso de usuarios y trazabilidad de valores de datos con histórico de al menos un mes.
	Excede los Requerimientos	Existe trazabilidad de acceso de usuarios y trazabilidad de valores de datos con histórico de más de un mes
Confidencialidad	Inaceptable	No implementa contraseñas seguras
	Mínimamente Aceptable	Implementa contraseñas seguras
	Rango Objetivo	Implementa cifrado de datos y contraseñas seguras
	Excede los Requerimientos	Implementa cifrado de datos, contraseñas seguras y otros mecanismos de seguridad del ENS
Disponibilidad (Nivel de servicio)	Inaceptable	Nivel de servicio inferior al 98,5%
	Mínimamente Aceptable	Nivel de servicio superior al 98,5%
	Rango Objetivo	Nivel de servicio superior al 99,5%
	Excede los Requerimientos	Nivel de servicio superior al 99,9%

Tabla 1: Criterios de decisión para la Calidad del Dato

Por lo último se definen los criterios de decisión para la evaluación final. Cada característica debe obtener como mínimo el valor definido a continuación:

Resultado Evaluación	Inaceptable	Recuperabilidad: Inaceptable Conformidad: Inaceptable Trazabilidad: Inaceptable Confidencialidad: Inaceptable Disponibilidad: Inaceptable
	Mínimamente Aceptable	Recuperabilidad: Mínimamente Aceptable Conformidad: Mínimamente Aceptable Trazabilidad: Mínimamente Aceptable Confidencialidad: Mínimamente Aceptable Disponibilidad: Mínimamente Aceptable
	Rango Objetivo	Recuperabilidad: Rango Objetivo Conformidad: Rango Objetivo Trazabilidad: Rango Objetivo

		Confidencialidad: Rango Objetivo Disponibilidad: Rango Objetivo
	Excede los Requerimientos	Recuperabilidad: Excede los Requerimientos Conformidad: Excede los Requerimientos Trazabilidad: Excede los Requerimientos Confidencialidad: Excede los Requerimientos Disponibilidad: Excede los Requerimientos

Tabla 2: Criterios de decisión para evaluación final para Calidad del Dato

3.10.3. Documentación previa requerida

Recuperabilidad (Informe de Recuperabilidad DQ) (Acreditación de recuperabilidad por parte de terceros)	En los sistemas propios el informe será elaborado por el responsable de sistemas. En los sistemas de terceros, ya se encuentren en cloud o en el propio CPD del Ayuntamiento, la empresa responsable tendrá que acreditar los tiempos de recuperabilidad, también se podrá emplear la experiencia previa del departamento de informática en procesos ya realizados.
Conformidad (Plan de adecuación al ENS, grado de cumplimiento del ENI, grado de cumplimiento del ENS) (Acreditación de certificaciones por parte de terceros)	En los sistemas propios el responsable de seguridad aportará los documentos necesarios para certificar el cumplimiento. En los sistemas de terceros, ya se encuentren en cloud o en el propio CPD del Ayuntamiento, la empresa responsable tendrá que acreditar todas las medidas implantadas así como mostrar las respectivas certificaciones.
Trazabilidad (Informe de Trazabilidad DQ) (Acreditación de trazabilidad por parte de terceros)	En los sistemas propios el informe será elaborado por el responsable de sistemas. En los sistemas de terceros, ya se encuentren en cloud o en el propio CPD del Ayuntamiento, la empresa responsable tendrá que demostrar cómo se realiza la trazabilidad.
Confidencialidad (Informe de Confidencialidad DQ)	El informe será elaborado por el responsable de sistemas.
Disponibilidad (Informe de Disponibilidad DQ) (ANS con los Proveedores)	El informe será elaborado por el responsable de sistemas.

Tabla 3: Documentación previa para evaluar la Calidad del Dato

3.11. Otra documentación

A pesar de que en este documento no vamos a elaborar toda la documentación requerida para el cumplimiento del ENS, RGPD y de ISO/IEC 27001:2013 vamos a documentarla de modo que cuando se realice la implantación real se disponga de ella o al menos de una referencia para evitar olvidos.

3.11.1. ISO/IEC 27001:2013

3.11.1.1. Obligatorios

Entre paréntesis agregamos el control ISO/IEC 27002:2013 donde se nombra:

1. Uso aceptable de los activos: buenas prácticas de uso, cubre un extenso rango de temas. (A.8.1.3)
2. Política de control de acceso: acceso a redes, documentación, información, sistemas, etc. ya sea tanto acceso físico como lógico. (A.9.1.1)
3. Procedimientos operativos para gestión de TI: define servicios a terceros, transferencia de información, tratamiento de códigos maliciosos o gestión del cambio, entre otros. (A.12.1.1)
4. Principios de ingeniería de seguridad: define entorno a las distintas secciones relacionadas con la ingeniería cómo se va a abordar la incorporación de las técnicas de seguridad (aplicaciones, negocio, tecnología y datos). (A.14.2.5)
5. Política de seguridad para proveedores: controles a proveedores desde el inicio en su contratación hasta el fin de la relación aunque aún no se haya producido. (A.15.1.1)
6. Procedimiento para la gestión de incidentes: establece cómo hay que documentar, informar, clasificar, notificar, contener, resolver, etc. un incidente de seguridad. (A.16.1.5)
7. Procedimientos de la continuidad del negocio: incluye planes para la continuidad del negocio, la respuesta ante incidentes que alarguen la interrupción del servicio, recuperaciones del sector comercial de la organización y Disaster Recovery. (A.17.1.2)
8. Registro de capacitación, habilidades, experiencia y calificaciones: documento orientado al registro del activo principal en RRHH, el empleado de la organización. (7.2)
9. Resultado de supervisión y medición: mide los indicadores clave de desempeño para realizar seguimientos, se tiene que reportar a los responsables de cada activo. (9.1)
10. Resultados de acciones correctivas: establece valores medibles sobre las acciones correctivas tomadas para poder evaluar lo adecuado de las acciones correctivas. (10.1)
11. Registros sobre actividades de los usuarios, excepciones y eventos de seguridad: tal y como indica el nombre es un registro de actividad, un log. (A.12.4.1 y A.12.4.3)

3.11.1.2. No obligatorios pero recomendables

1. Procedimiento para el control de documentos y documento de controles para gestión de registros: se debe escribir el primero de todos los documentos y establece como se va a manejar la información en el resto de documentos y registros. (7.5)
2. Procedimiento para medidas correctivas: establece cómo se van a llevar a cabo (fases, pasos) las medidas correctivas. Es habitual ponerlo en conocimiento de los empleados. (10.1)
3. Política trae tu dispositivo (BYOD): establece los controles al acceder desde un dispositivo no corporativo a la información de la empresa. (A.6.2.1)
4. Política sobre dispositivos móviles y teletrabajo: para evitar el acceso no autorizado. (A.6.2.1)
5. Política de clasificación de la información: confidencial, pública, interna a la organización, etc. (A.8.2.1, A.8.2.2 y A.8.2.3)
6. Política de claves: reglas a la hora de establecer contraseñas (A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3)
7. Política de eliminación y destrucción: garantizarla de manera segura. (A.8.3.2 y A.11.2.7)
8. Procedimiento para trabajo en áreas seguras: para tareas con riesgos, ejemplo manipulación de baterías o fuentes de alimentación. (A.11.1.5)
9. Política de pantalla y escritorio limpio: para evitar accesos no autorizados ante puestos de trabajo desatendidos. (A.11.2.9)
10. Política de gestión del cambio: controla y gestiona los cambios en los sistemas de información. (A.12.1.2 y A.14.2.4)
11. Política de creación de copias de seguridad: tipo de copia (completa, incremental) y frecuencia. Soportes. Ubicación. (A.12.3.1)
12. Política de transferencia de la información: seguridad de la información y el software cuando se intercambian fuera o dentro de la empresa. (A.13.2.1, A.13.2.2, y A.13.2.3)
13. Plan de prueba y verificación: evalúa las medidas y acciones correctivas. (A.17.1.3)
14. Plan de mantenimiento y revisión: periodicidad para la revisión y mantenimiento del sistema de gestión, relacionado con ISO 22301. (cláusula 17.1.3)

3.11.2. Esquema Nacional de Seguridad

1. Plan anual de difusión/sensibilización y de formación.
2. Procedimiento de gestión de la seguridad con terceros.
3. Procedimiento de Protección frente a código dañino.
4. Procedimiento de Segmentación de redes.
5. Procedimiento de control de acceso.
6. Política de acceso a información.
7. Instrucciones Técnicas de Configuración Segura.
8. Procedimiento de copias de Seguridad
9. Procedimiento integral de gestión de incidentes de seguridad.
10. Procedimiento de acceso y seguridad física del CPD.

11. Procedimiento de captura de registros de actividad.
12. Procedimiento de pruebas a realizar antes de la puesta en producción de las aplicaciones.
13. Normativa de acceso remoto.
14. Procedimiento de autenticación por recurso.
15. Política de uso seguro de contraseñas.
16. Procedimientos operativos de seguridad sobre el sistema.
17. Procedimiento de autorización para la introducción de elementos en el sistema.
18. Arquitectura de seguridad.
19. Procedimiento de análisis de riesgos para la adquisición de nuevos componentes.
20. Procedimiento de dimensionamiento y gestión de la capacidad.
21. Procedimiento de asignación de tareas.
22. Procedimiento de inventario de activos.
23. Procedimiento de mantenimiento.
24. Procedimiento de gestión de cambios de proveedores.
25. Normativa de seguridad de claves criptográficas.
26. Sistema de métricas.
27. Procedimiento de inventario de áreas con acceso al sistema de información.
28. Medidas de garantía de suministro eléctrico.
29. Procedimiento de protección frente a incendios.
30. Procedimiento de deberes y obligaciones de la plantilla municipal.
31. Documentación sobre seguridad perimetral.
32. Procedimiento de protección de la confidencialidad.
33. Procedimiento de protección de la autenticidad y la integridad.
34. Procedimiento de etiquetado de soportes de información extraíbles.
35. Procedimiento de custodia de soportes de información.
36. Procedimiento de protección de soportes de información durante el transporte.
37. Procedimiento de borrado y destrucción de soportes de información.
38. Procedimiento de calificación de la información.
39. Política de firma electrónica y certificados.
40. Procedimiento sobre los requisitos de los sellos de tiempo.
41. Procedimiento para la limpieza de documentos electrónicos.
42. Procedimiento de protección del correo electrónico.
43. Documentación de medidas de prevención ante ataques DDoS.
44. Política de gestión documental.
45. Acta de Aceptación de Riesgos por parte de la Dirección.

3.11.3. RGPD / LOPDGDD

1. Registro de actividades de tratamiento.
2. Procedimiento de designación del DPD.
3. Análisis de riesgos adaptado al RGPD.
4. Evaluación de impacto.
5. Contrato de encargado de tratamiento.
6. Procedimiento de alineamiento de medidas de seguridad con las del ENS.
7. Política de Protección de Datos.

4. Análisis de Riesgos

4.1. Análisis de Riesgos

Se lleva a cabo el análisis de riesgos con la metodología MAGERIT mediante el empleo de la herramienta PILAR del Centro Criptológico Nacional [33], de la que se nos cede una versión con licencia educativa para poder realizar este trabajo. Todos los datos han sido obtenidos mediante el empleo de los informes de la herramienta.

Es de notar la ausencia de muchos activos, como por ejemplo las interfaces de comunicación entre los distintos elementos del CPD ó software de gestión de infraestructura, esto es debido a que quedaba fuera del alcance de este TFM por escasez de tiempo el análisis exhaustivo del entorno, el cual deberá ser realizado en el Ayuntamiento real de referencia. Con todo, se ha recreado un entorno de activos que abarca lo esencial y con una variedad suficiente para obtener todos los posibles impactos y riesgos asociados a nuestro sistema de información, por lo que se obtendrán resultados muy aproximados a la realidad.

4.1.1. Inventario de Activos

Se han agrupado los activos de forma acorde a la metodología MAGERIT, en este caso distinguimos los siguientes: Instalaciones [L], Aplicación [SW], Servicios [S], Equipamiento Auxiliar [AUX], Hardware [HW], Red [COM], Personal [P] y Datos [D].

Con el objetivo de poder obtener informes más detallados y más claros se han creado dentro de estas agrupaciones contenedores de objetos que engloban conjuntos de activos relacionados.

En total se han identificado los siguientes activos, se destacan en negrita los contenedores de objetos, sin resaltar quedan los activos:

Capa: [L] Instalaciones

[L.building_CC] Casa Consistorial
[L.building_CP] Centro Polivalente
[L.local_CPD] CPD Casa Consistorial
[L.building_SP] Satélite Policía
[L.ST] Servicios Técnicos
[L.building_ST] Servicios Técnicos
[L.channel_fibraST] Fibra Servicios Técnicos Casa Consistorial

[L.BIBLIO] Biblioteca
[L.building_Biblioteca] Biblioteca
[L.channel_fibraB] Fibra Biblioteca Casa Consistorial

Capa: [SW] Aplicación

[SW.Aplicaciones] Servidores de Aplicaciones
[SW.APP.Padron] WPadron
[SW.APP.Eurocop] Eurocop Servidor
[SW.APP.Nominas] A3Nom
[SW.APP.GLPI] Gestion Informática GLPI
[SW.APP.Impresion] Servidor Impresión MyQ
[SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo
[SW.www.Intranet] Servicio Intranet Local
[SW.office] Software Ofimática
[SW.office.Libre7] LibreOffice7
[SW.office.Office13ADV] Office 2013 advanced
[SW.office.Office13STA] Office 2013 standard
[SW.Clientes] Software Cliente
[SW.Other.Padron] Padrón Cliente
[SW.Other.Eurocop] Eurocop Cliente
[SW.Other.Lexnet] Lexnet Cliente
[SW.Other.Siltra] Siltra Cliente
[SW.Other.ZKSoft] ZkSoftware Cliente Control Accesos
[SW.Other.GIS] Software de Gestión Territorial Cliente
[SW.Other.Reca] ATM Recaudación Cliente
[SW.Other.VNC] VNC Cliente
[SW.Other.Conta] ATM Contabilidad Cliente
[SW.Other.AutoCAD19] Software Autocad 2019
[SW.Other.Presto] Software Presto 2019
[SW.Other.SondaProveedor] Sonda Servicio Proveedor Mantenimiento
[SW.Cloud] Software en Cloud
[SW.email_server.Postfix] Servidor Correo
[SW.www.Plesk_1] Servidor Plesk Correo
[SW.www.Plesk_2] Servidor Plesk Web
[SW.www.WebAyto] Servicio Wordpress
[SW.Pruebas] Servidores Pruebas
[SW.Other.Pruebas_2] Servidor Pruebas
[SW.Other.Pruebas_3] Servidor Pruebas
[SW.Other.Pruebas_1] Servidor Pruebas
[SW.Virtualización] Virtualización de Infraestructura y Escritorios
[SW.APP.VDIConnection_1] Servidor VDI Connection
[SW.APP.VDIConnection_3] Servidor VDI Connection
[SW.APP.VDIConnection_2] Servidor VDI Connection
[SW.APP.VDIComposer] Servidor VDI Composer
[SW.APP.VDISecurity] Servidor VDI Security
[SW.file.PerfilesVDI] Servidor ficheros de Perfiles VDI
[SW.hypervisor.Horizon7] Horizon VDI
[SW.hypervisor.vCenterInfra] vCenter Infraestructura
[SW.hypervisor.vCenterVDI] vCenter VDI
[SW.infra] Software de Infraestructura

[SW.directory.DC_1] Controlador Dominio DNS
[SW.directory.DC_2] Controlador Dominio DNS
[SW.directory.DHCP_1] Servidor DHCP
[SW.directory.DHCP_2] Servidor DHCP
[SW.APP.KMS] Servidor Licencias Microsoft
[SW.APP.WSUS] Servidor Actualizaciones Microsoft
[SW.file.Ficheros] Servidor de Ficheros
[SW.Other.Santricity] Gestor de Storage

[SW.backup] Software de Backup

[SW.backup.Backup_1] Servidor VDP Backup
[SW.backup.Backup_2] Servidor VDP Backup

[SW.dbms.SQL12] Servidor SQL Server 2012

[SW.seguridad] Software de seguridad

[SW.AV.SophosServer] Sophos Advanced Server
[SW.AV.SophosFisicos] Sophos Standard Equipos Físicos
[SW.AV.SophosVDI] Sophos Advanced VDI
[SW.APP.ServerEndpoint_2] Servidor Sophos Endpoint
[SW.APP.ServerEndpoint_1] Servidor Sophos Endpoint

[SW.OS.WIN12] Server 2012 R2
[SW.OS.WIN16] Server 2016 VDI
[SW.OS.WIN10] Windows 10
[SW.OS.CENT7] Server Linux Centos 7

Capa: [S] Servicios

[S.cloud.SophosCentral] Central Endpoint Cloud de Sophos
[S.other.Mantenimiento] Mantenimiento para el CPD
[S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes
[S.iaas.MailWeb] Proveedor de Infraestructura como Servicio
[S.ca.Certs] Proveedor de certificados FNMT
[S.other.Soporte] Proveedores de soporte de aplicaciones
[S.isp.Internet] Proveedor de acceso a Internet

Capa: [AUX] Equipamiento Auxiliar

[AUX.CPD] elementos del CPD

[AUX.ups.CPD_2] UPS del CPD
[AUX.ac.CPD_2] Split de Aire Acondicionado del CPD
[AUX.furniture.RackCPD_2] Rack CPD
[AUX.furniture.RackCPD_1] Rack CPD
[AUX.furniture.Armario] Armario Ignífugo Caja Fuerte
[AUX.ac.CPD_1] Split de Aire Acondicionado del CPD
[AUX.ups.CPD_1] UPS del CPD
[AUX.other.Extintor] Extintor de CO2
[AUX.other.AccesoCPD] Sistema de control de acceso con alarma al CPD

[AUX.ups.SatPolicia] Mini UPS del Satélite de Policía
[AUX.ups.CentroPol] Mini UPS del Centro Polivalente

Capa: [HW] Hardware

[HW.CPD] Equipos del CPD

[HW.CPD.INFRA] HW Virtualización Equipos Infraestructura
[HW.host.INFRA_2] ESX Infraestructura
[HW.host.INFRA_1] ESX Infraestructura
[HW.data.CabinaProd] Cabina de Producción
[HW.vhost.Switch] Switch Virtual Servidores Infraestructura
[HW.data.DataStores_3] DataStores Virtuales Equipos Infraestructura
[HW.data.DataStores_2] DataStores Virtuales Backup
[HW.data.CabinaBack] Cabina de Backup
[HW.vhost.Servidores] Máquinas Virtuales Servidores Infraestructura
[HW.CPD.VDI] Hardware Virtualización de Escritorios
[HW.host.VDI_2] ESX VDI
[HW.host.VDI_3] ESX VDI
[HW.host.VDI_1] ESX VDI
[HW.data.DataStores_1] DataStores Virtuales Escritorios Usuarios vSAN
[HW.vhost.Switch_1] Switch Virtual Escritorios Usuarios
[HW.vhost.VDI] Máquinas Virtuales Escritorios Usuarios
[HW.CPD.COM] Comunicaciones CPD
[HW.other.Firewall_2] Firewall en HA
[HW.other.Firewall_1] Firewall en HA
[HW.Other.SwitchStack] Core Switch Stack 10G
[HW.switch.SwitchCPD_2] Switch de Usuario CPD
[HW.switch.SwitchCPD_1] Switch de Usuario CPD
[HW.router.CPD_2] Router ADSL Servicio Correo Postal
[HW.router.CPD_3] Router ADSL Red SARA
[HW.router.CPD_1] Router Fibra Principal CPD
[HW.CentroPol] Equipos Centro Polivalente
[HW.other.MiniFW_2] Firewall Centro Polivalente
[HW.router.CentroPol] Router Fibra Centro Polivalente
[HW.switch.SwitchST] Switch de Usuario Servicios Técnicos
[HW.SatPolicia] Equipos Satélite Policia
[HW.router.SatPolicia] Router Fibra Satélite Policiía
[HW.other.MiniFW_1] Firewall Satélite Policía
[HW.switch.SwitchCCP2] Switch de Usuario Casa Consistorial P2
[HW.switch.SwitchBiblio] Switch de Usuario Biblioteca
[HW.pc.ZeroClient] Equipos de Usuarios Virtualizados
[HW.pc.Equipo] Equipos de Usuarios
[HW.mobile.PortatilTeletrabajo] Equipo Portátil para Teletrabajo
[HW.print.Impresoras] Impresoras
[HW.vhost.Cloud] Máquinas Virtuales Servidores Infraestructura Cloud

Capa: [COM] Red

[COM.CentroPol] Comunicaciones Centro Polivalente
[COM.other.CentroPol] Túnel Centro Polivalente CPD
[COM.wan.CentroPol] WAN del Centro Polivalente
[COM.SatPolicia] Comunicaciones Satélite Policía
[COM.other.SatPolicia] Túnel Satélite Policía CPD
[COM.wan.SatPolicia] WAN del Satélite Policía
[COM.CPD] Comunicaciones CPD
[COM.vpn.RedSara] VPN con la Red Sara
[COM.other.Teletrabajo] Conexión contra servidor de seguridad PCoIP

[COM.vpn.RedMonitor] VPN con la Red de Monitorización para mantenimiento
[COM.adsl.CPD_2] ADSL Correos Postal IP fija
[COM.wan.CPD] WAN del CPD
[COM.vlan.ILO] VLAN para las ilos de los hosts
[COM.vlan.VSAN] VLAN para el servicio de vSAN
[COM.adsl.CPD_1] ADSL Red Sara IP fija
[COM.vlan.EquiposInfra] VLAN para los Equipos de Infraestructura
[COM.vlan.EquiposUsuario] VLAN para los usuarios de Usuario Interno
[COM.vlan.EquiposMancomunidad] VLAN para los usuarios de la Mancomunidad

Capa: [P] Personal

[P.ui.Oper] Usuarios Operadores del Sistema
[P.prov] Usuarios Proveedores
[P.prov.Oper] Usuarios Proveedores Operadores del Sistema
[P.prov.Admins] Usuarios Proveedores Administradores del Sistema
[P.adm.Admins] Usuarios Administradores del Sistema
[P.ui.UsuInternos] Usuarios Internos
[P.ue.Oposicion] Usuarios miembros de la Oposición Política
[P.ue.Mancomunidad] Usuarios de la Mancomunidad

Capa: [D] Datos

[D.Virtualizacion] Datos relacionados con la Virtualización
[D.conf.Virtualización] BD de los vCenters
[D.files.PerfilesVDI] Datos de los Escritorios de VDI
[D.conf.PlantillasVDI] Plantillas VDI
[D.logs.VDI] Logs de los vCenters y Horizon
[D.files.ServFicheros] Datos en Unidades de Red Compartidas
[D.backup.Respaldos] Datos de las copias de Seguridad
[D.BDSQLServer] BD contenidas en el servidor de SQL
[D.files.BD_Contabilidad] BD Aplicación Contabilidad
[D.files.BD_Recaudacion] BD Aplicación Recaudación
[D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos
[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo
[D.files.BD_GIS] BD Aplicación GIS
[D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware
[D.files.BD_Padron] BD Aplicación WPadron
[D.files.BD_Nominas] BD Aplicación A3Nom
[D.conf.GPO] Datos de configuración de las GPOs
[D.files.BD_Eurocop] BD Aplicación Eurocop
[D.logs.Windows] Logs de Windows

Consideraremos **activo esencial** todo aquel que contenga datos de carácter personal como veremos en el punto 4.2.3.

4.1.2. Dependencias entre Activos

Dentro de la herramienta PILAR podemos jerarquizar los activos de modo que si un activo contiene o depende de otro podamos sumar el riesgo de materialización de una amenaza a este, por lo que vamos a definir una estructura padre-hijo. Si bien se podría haber profundizado mucho más en el modelo de dependencia se ha optado por uno más simplificado para evitar la excesiva propagación de valores y la situación del "todo es muy importante" de lo contrario hasta el extintor de CO2 del CPD hubiese obtenido valores críticos en confidencialidad por ejemplo.

De forma esquemática la relación entre agrupaciones de activos ha quedado del siguiente modo:

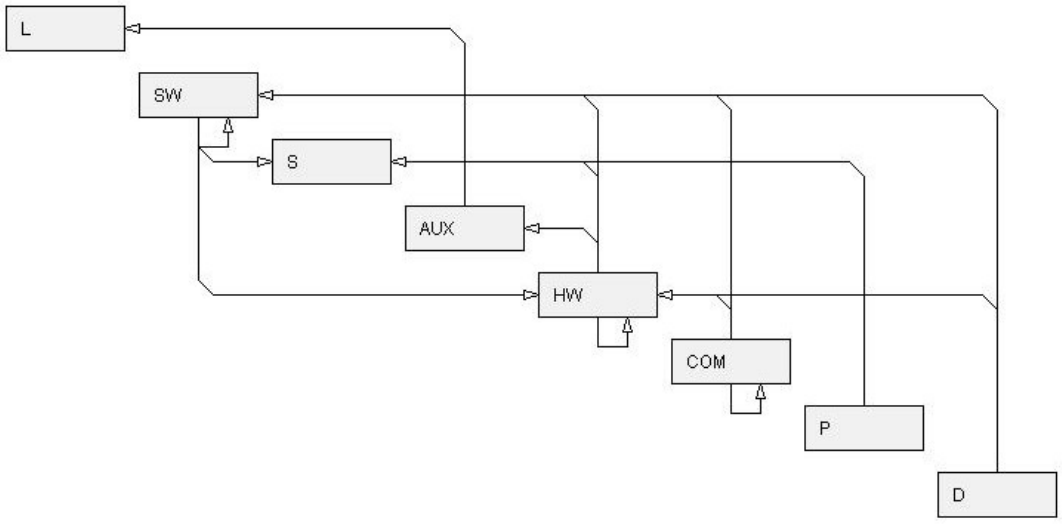

Figura 8 - Relaciones entre tipos de activos

Para visualizar la relación completa entre activos, se puede utilizar el siguiente producto obtenido en el TFM, aunque para una visualización más interactiva y clara es recomendable utilizar la herramienta PILAR y cargar el proyecto al completo:

Ver producto obtenido del TFM (Relación entre activos.jpg)

Si bien en el punto 4.2.3. de valoración no se reflejan los valores acumulados por las dependencias, la herramienta PILAR sí que utiliza estos valores para el cálculo posterior del impacto potencial y el riesgo. Ejemplo de aplicación:

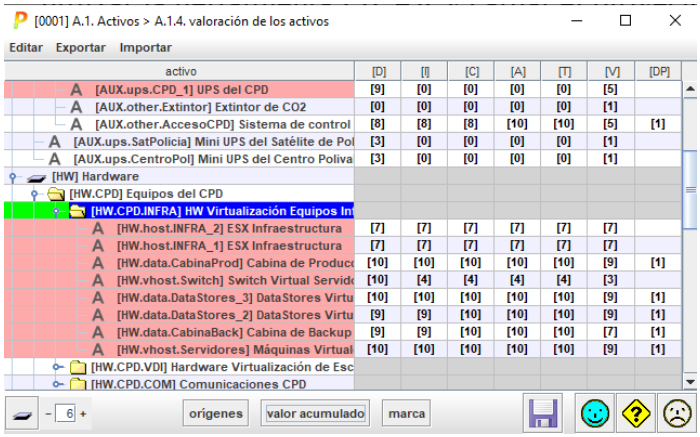

Figura 9 - Ejemplo de valoración de activo propia

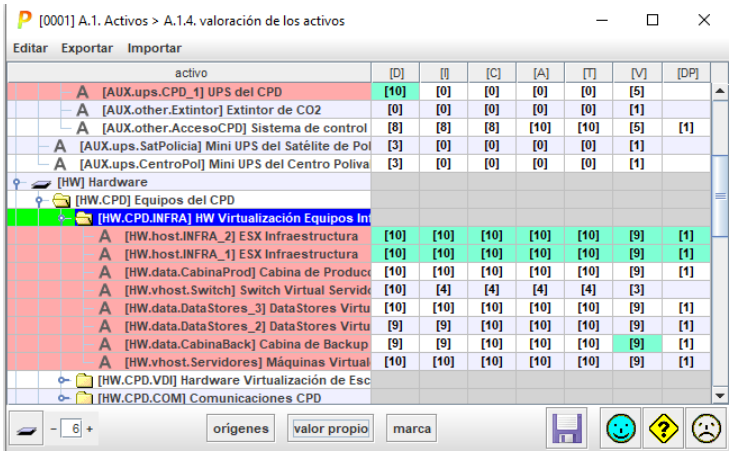

Figura 10 - Ejemplo de valoración de activo acumulada

4.1.3. Valoración de los Activos, Valoración ACIDA y Valoración Datos Personales (RGPD)

Incluimos todas las valoraciones en una misma tabla por comodidad, donde la valoración ACIDA correspondería a las cinco primeras columnas, la valoración del activo sería la sexta columna y finalmente si el activo contiene datos personales (convirtiéndose en activo esencial). Significado de las columnas:

- D: valoración de disponibilidad de los datos.
- I: valoración de integridad de los datos.
- C: valoración de confidencialidad de los datos.
- A: autenticidad de los usuarios y la información.
- T: trazabilidad del servicio y de los datos.
- V: valoración del activo, siendo 9 equivalente a valor Muy alto para la organización, 7 equivalente a Alto, 5 equivalente a Medio, 3 equivalente a Bajo y 1 equivalente a Muy bajo.
- DP: datos personales, siendo el valor 1 indicativo de que el activo contiene datos personales.

capa: [L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L.building_CC] Casa Consistorial	[10]	[8]	[8]	[5]	[5]	[9]	[1]
[L.building_CP] Centro Polivalente	[3]	[3]	[3]	[5]	[5]	[9]	
[L.local_CPD] CPD Casa Consistorial	[10]	[8]	[8]	[10]	[10]	[9]	[1]
[L.building_SP] Satélite Policía	[3]	[3]	[3]	[5]	[5]	[7]	
[L.building_ST] Servicios Técnicos	[5]	[3]	[5]	[5]	[5]	[9]	[1]
[L.channel_fibraST] Fibra Servicios Técnicos Casa Consistorial	[5]	[3]	[5]	[2]	[2]	[3]	
[L.building_Biblioteca] Biblioteca	[1]	[1]	[1]	[2]	[5]	[9]	
[L.channel_fibraB] Fibra Biblioteca Casa Consistorial	[1]	[1]	[1]	[1]	[1]	[3]	

Tabla 4: AR - Valoración Activos Instalaciones

capa: [SW] Aplicación

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW.APP.Padron] WPadron	[8]	[10]	[10]	[10]	[10]	[7]	[1]
[SW.APP.Eurocop] Eurocop Servidor	[6]	[9]	[10]	[10]	[10]	[7]	[1]
[SW.APP.Nominas] A3Nom	[6]	[9]	[10]	[10]	[10]	[7]	[1]
[SW.APP.GLPI] Gestion Informatica GLPI	[3]	[6]	[5]	[8]	[8]	[5]	
[SW.APP.Impresion] Servidor Impresión MyQ	[3]	[3]	[3]	[3]	[5]	[5]	
[SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo	[4]	[6]	[10]	[8]	[10]	[5]	[1]
[SW.www.Intranet] Servicio Intranet Local	[3]	[5]	[10]	[5]	[5]	[3]	[1]
[SW.office.Libre7] LibreOffice7	[2]	[2]	[2]	[1]	[2]	[1]	
[SW.office.Office13ADV] Office 2013 advanced	[2]	[2]	[2]	[1]	[2]	[3]	
[SW.office.Office13STA] Office 2013 standard	[2]	[2]	[2]	[1]	[2]	[3]	
[SW.Other.Padron] Padrón Cliente	[1]	[1]	[3]	[10]	[1]	[1]	[1]
[SW.Other.Eurocop] Eurocop Cliente	[1]	[1]	[3]	[10]	[1]	[1]	[1]
[SW.Other.Lexnet] Lexnet Cliente	[1]	[1]	[5]	[10]	[1]	[1]	[1]
[SW.Other.Siltra] Siltra Cliente	[1]	[1]	[3]	[10]	[1]	[1]	[1]
[SW.Other.ZKSoft] ZkSoftware Cliente Control Accesos	[1]	[1]	[3]	[3]	[1]	[1]	[1]
[SW.Other.GIS] Software de Gestión Territorial Cliente	[7]	[7]	[3]	[5]	[1]	[5]	[1]
[SW.Other.Reca] ATM Recaudación Cliente	[1]	[1]	[3]	[10]	[1]	[1]	[1]
[SW.Other.VNC] VNC Cliente	[1]	[1]	[3]	[7]	[3]	[1]	
[SW.Other.Conta] ATM Contabilidad Cliente	[1]	[1]	[3]	[10]	[1]	[1]	[1]

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW.Other.AutoCAD19] Software Autocad 2019	[2]	[2]	[2]	[2]	[2]	[5]	
[SW.Other.Presto] Software Presto 2019	[2]	[2]	[2]	[2]	[2]	[3]	
[SW.Other.SondaProveedor] Sonda Servicio Proveedor Mantenimiento	[2]	[2]	[2]	[5]	[5]	[3]	
[SW.email_server.Postfix] Servidor Correo	[8]	[9]	[10]	[10]	[10]	[7]	[1]
[SW.www.Plesk_1] Servidor Plesk Correo	[8]	[9]	[5]	[7]	[7]	[5]	[1]
[SW.www.Plesk_2] Servidor Plesk Web	[8]	[9]	[5]	[7]	[7]	[5]	
[SW.www.WebAyto] Servicio Wordpress	[8]	[9]	[5]	[10]	[10]	[7]	
[SW.Other.Pruebas_2] Servidor Pruebas	[0]	[0]	[5]	[5]	[0]	[1]	
[SW.Other.Pruebas_3] Servidor Pruebas	[0]	[0]	[5]	[5]	[0]	[1]	
[SW.Other.Pruebas_1] Servidor Pruebas	[0]	[0]	[5]	[5]	[0]	[1]	[1]
[SW.APP.VDIConnection_1] Servidor VDI Connection	[7]	[3]	[3]	[7]	[7]	[7]	
[SW.APP.VDIConnection_3] Servidor VDI Connection	[7]	[3]	[3]	[7]	[7]	[7]	
[SW.APP.VDIConnection_2] Servidor VDI Connection	[7]	[3]	[3]	[7]	[7]	[7]	
[SW.APP.VDIComposer] Servidor VDI Composer	[2]	[3]	[3]	[3]	[5]	[3]	
[SW.APP.VDISecurity] Servidor VDI Security	[7]	[3]	[5]	[10]	[10]	[7]	
[SW.file.PerfilesVDI] Servidor ficheros de Perfiles VDI	[7]	[9]	[10]	[10]	[10]	[9]	[1]
[SW.hypervisor.Horizon7] Horizon VDI	[3]	[3]	[3]	[7]	[7]	[7]	
[SW.hypervisor.vCenterInfra] vCenter Infraestructura	[3]	[3]	[3]	[7]	[7]	[7]	
[SW.hypervisor.vCenterVDI] vCenter VDI	[3]	[3]	[3]	[7]	[7]	[7]	
[SW.directory.DC_1] Controlador Dominio DNS	[7]	[8]	[7]	[10]	[10]	[7]	[1]
[SW.directory.DC_2] Controlador Dominio DNS	[7]	[8]	[7]	[10]	[10]	[7]	[1]
[SW.directory.DHCP_1] Servidor DHCP	[7]	[3]	[3]	[7]	[10]	[7]	
[SW.directory.DHCP_2] Servidor DHCP	[7]	[3]	[3]	[7]	[10]	[7]	
[SW.APP.KMS] Servidor Licencias Microsoft	[2]	[3]	[5]	[5]	[5]	[5]	
[SW.APP.WSUS] Servidor Actualizaciones Microsoft	[2]	[2]	[2]	[2]	[2]	[7]	
[SW.file.Ficheros] Servidor de Ficheros	[9]	[9]	[10]	[10]	[10]	[9]	[1]
[SW.Other.Santricity] Gestor de Storage	[0]	[0]	[0]	[7]	[0]	[1]	
[SW.backup.Backup_1] Servidor VDP Backup	[6]	[9]	[7]	[10]	[10]	[7]	
[SW.backup.Backup_2] Servidor VDP Backup	[6]	[9]	[7]	[10]	[10]	[7]	
[SW.dbms.SQL12] Servidor SQL Server 2012	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[SW.AV.SophosServer] Sophos Advanced Server	[8]	[8]	[8]	[10]	[10]	[7]	

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW.AV.SophosFisicos] Sophos Standard Equipos Físicos	[6]	[6]	[6]	[8]	[8]	[5]	
[SW.AV.SophosVDI] Sophos Advanced VDI	[6]	[6]	[6]	[8]	[8]	[7]	
[SW.APP.ServerEndpoint_2] Servidor Sophos Endpoint	[8]	[8]	[8]	[10]	[10]	[7]	
[SW.APP.ServerEndpoint_1] Servidor Sophos Endpoint	[8]	[8]	[8]	[10]	[10]	[7]	
[SW.OS.WIN12] Server 2012 R2	[5]	[5]	[5]	[5]	[5]	[5]	
[SW.OS.WIN16] Server 2016 VDI	[2]	[2]	[2]	[5]	[5]	[3]	
[SW.OS.WIN10] Windows 10	[2]	[2]	[2]	[5]	[5]	[1]	
[SW.OS.CENT7] Server Linux Centos 7	[8]	[9]	[8]	[8]	[8]	[3]	[1]

Tabla 5: AR - Valoración Activos Aplicación

capa: [S] Servicios

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[S.cloud.SophosCentral] Central Endpoint Cloud de Sophos	[8]	[8]	[8]	[10]	[10]	[7]	
[S.other.Mantenimiento] Mantenimiento para el CPD	[7]	[3]	[3]	[3]	[9]	[7]	
[S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[S.iaas.MailWeb] Proveedor de Infraestructura como Servicio	[9]	[9]	[10]	[10]	[10]	[9]	[1]
[S.ca.Certs] Proveedor de certificados FNMT	[6]	[6]	[6]	[10]	[6]	[5]	
[S.other.Soporte] Proveedores de soporte de aplicaciones	[2]	[3]	[5]	[2]	[2]	[3]	
[S.isp.Internet] Proveedor de acceso a Internet	[10]	[2]	[2]	[2]	[5]	[9]	

Tabla 6: AR - Valoración Activos Servicios

capa: [AUX] Equipamiento Auxiliar

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX.ups.CPD_2] UPS del CPD	[9]	[0]	[0]	[0]	[0]	[5]	
[AUX.ac.CPD_2] Split de Aire Acondicionado del CPD	[7]	[0]	[0]	[0]	[0]	[5]	
[AUX.furniture.RackCPD_2] Rack CPD	[7]	[0]	[0]	[0]	[0]	[5]	
[AUX.furniture.RackCPD_1] Rack CPD	[7]	[0]	[0]	[0]	[0]	[5]	
[AUX.furniture.Armario] Armario Ignífugo Caja Fuerte	[0]	[3]	[8]	[8]	[0]	[5]	

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX.ac.CPD_1] Split de Aire Acondicionado del CPD	[7]	[0]	[0]	[0]	[0]	[5]	
[AUX.ups.CPD_1] UPS del CPD	[9]	[0]	[0]	[0]	[0]	[5]	
[AUX.other.Extintor] Extintor de CO2	[0]	[0]	[0]	[0]	[0]	[1]	
[AUX.other.AccesoCPD] Sistema de control de acceso con alarma al CPD	[8]	[8]	[8]	[10]	[10]	[5]	[1]
[AUX.ups.SatPolicia] Mini UPS del Satélite de Policía	[3]	[0]	[0]	[0]	[0]	[1]	
[AUX.ups.CentroPol] Mini UPS del Centro Polivalente	[3]	[0]	[0]	[0]	[0]	[1]	

Tabla 7: AR - Valoración Activos Equipamiento Auxiliar

capa: [HW] Hardware

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW.host.INFRA_2] ESX Infraestructura	[7]	[7]	[7]	[7]	[7]	[7]	
[HW.host.INFRA_1] ESX Infraestructura	[7]	[7]	[7]	[7]	[7]	[7]	
[HW.data.CabinaProd] Cabina de Producción	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[HW.vhost.Switch] Switch Virtual Servidores Infraestructura	[10]	[4]	[4]	[4]	[4]	[3]	
[HW.data.DataStores_3] DataStores Virtuales Equipos Infraestructura	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[HW.data.DataStores_2] DataStores Virtuales Backup	[9]	[9]	[10]	[10]	[10]	[9]	[1]
[HW.data.CabinaBack] Cabina de Backup	[9]	[9]	[10]	[10]	[10]	[7]	[1]
[HW.vhost.Servidores] Máquinas Virtuales Servidores Infraestructura	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[HW.host.VDI_2] ESX VDI	[6]	[5]	[5]	[7]	[7]	[7]	[1]
[HW.host.VDI_3] ESX VDI	[6]	[5]	[5]	[7]	[7]	[7]	[1]
[HW.host.VDI_1] ESX VDI	[6]	[5]	[5]	[7]	[7]	[7]	[1]
[HW.data.DataStores_1] DataStores Virtuales Escritorios Usuarios vSAN	[7]	[7]	[10]	[10]	[10]	[9]	[1]
[HW.vhost.Switch_1] Switch Virtual Escritorios Usuarios	[7]	[4]	[4]	[4]	[4]	[3]	
[HW.vhost.VDI] Máquinas Virtuales Escritorios Usuarios	[2]	[2]	[7]	[7]	[7]	[5]	[1]
[HW.other.Firewall_2] Firewall en HA	[9]	[9]	[9]	[10]	[10]	[7]	
[HW.other.Firewall_1] Firewall en HA	[9]	[9]	[9]	[10]	[10]	[7]	
[HW.Other.SwitchStack] Core Switch Stack 10G	[10]	[4]	[4]	[7]	[7]	[7]	

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW.switch.SwitchCPD_2] Switch de Usuario CPD	[6]	[4]	[4]	[7]	[7]	[5]	
[HW.switch.SwitchCPD_1] Switch de Usuario CPD	[6]	[4]	[4]	[7]	[7]	[5]	
[HW.router.CPD_2] Router ADSL Servicio Correo Postal	[2]	[4]	[4]	[7]	[4]	[1]	
[HW.router.CPD_3] Router ADSL Red SARA	[4]	[4]	[4]	[7]	[4]	[3]	
[HW.router.CPD_1] Router Fibra Principal CPD	[9]	[4]	[4]	[7]	[4]	[5]	
[HW.other.MiniFW_2] Firewall Centro Polivalente	[3]	[9]	[9]	[10]	[10]	[3]	
[HW.router.CentroPol] Router Fibra Centro Polivalente	[3]	[4]	[4]	[7]	[4]	[1]	
[HW.switch.SwitchST] Switch de Usuario Servicios Técnicos	[6]	[4]	[4]	[7]	[7]	[5]	
[HW.router.SatPolicia] Router Fibra Satélite Policía	[3]	[4]	[4]	[7]	[4]	[1]	
[HW.other.MiniFW_1] Firewall Satélite Policía	[3]	[9]	[9]	[10]	[10]	[3]	
[HW.switch.SwitchCCP2] Switch de Usuario Casa Consistorial P2	[6]	[4]	[4]	[7]	[7]	[5]	
[HW.switch.SwitchBiblio] Switch de Usuario Biblioteca	[3]	[4]	[4]	[7]	[7]	[3]	
[HW.pc.ZeroClient] Equipos de Usuarios Virtualizados	[1]	[1]	[1]	[7]	[7]	[1]	
[HW.pc.Equipo] Equipos de Usuarios	[2]	[2]	[5]	[7]	[7]	[3]	[1]
[HW.mobile.PortatilTeletrabajo] Equipo Portátil para Teletrabajo	[2]	[2]	[5]	[2]	[7]	[3]	
[HW.print.Impresoras] Impresoras	[5]	[2]	[5]	[5]	[5]	[3]	
[HW.vhost.Cloud] Máquinas Virtuales Servidores Infraestructura Cloud	[8]	[9]	[9]	[10]	[10]	[8]	[1]

Tabla 8: AR - Valoración Activos Hardware

capa: [COM] Red

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[COM.other.CentroPol] Túnel Centro Polivalente CPD	[3]	[9]	[9]	[9]	[4]	[1]	
[COM.wan.CentroPol] WAN del Centro Polivalente	[3]	[4]	[4]	[4]	[4]	[1]	
[COM.other.SatPolicia] Túnel Satélite Policía CPD	[3]	[9]	[9]	[9]	[4]	[1]	
[COM.wan.SatPolicia] WAN del Satélite Policía	[3]	[4]	[4]	[4]	[4]	[1]	
[COM.vpn.RedSara] VPN con la Red Sara	[4]	[7]	[10]	[10]	[10]	[3]	[1]

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[COM.other.Teletrabajo] Conexión contra servidor de seguridad PCoIP	[7]	[7]	[7]	[10]	[10]	[3]	
[COM.vpn.RedMonitor] VPN con la Red de Monitorización para mantenimiento	[2]	[4]	[4]	[4]	[10]	[3]	
[COM.adsl.CPD_2] ADSL Correos Postal IP fija	[2]	[4]	[7]	[2]	[2]	[1]	
[COM.wan.CPD] WAN del CPD	[9]	[7]	[4]	[2]	[4]	[3]	
[COM.vlan.ILO] VLAN para las ilos de los hosts	[2]	[4]	[2]	[7]	[4]	[1]	
[COM.vlan.VSAN] VLAN para el servicio de vSAN	[6]	[4]	[2]	[4]	[4]	[5]	
[COM.adsl.CPD_1] ADSL Red Sara IP fija	[4]	[4]	[4]	[2]	[4]	[3]	
[COM.vlan.EquiposInfra] VLAN para los Equipos de Infraestructura	[10]	[10]	[10]	[10]	[10]	[5]	[1]
[COM.vlan.EquiposUsuario] VLAN para los usuarios de Usuario Interno	[9]	[9]	[9]	[7]	[7]	[3]	[1]
[COM.vlan.EquiposMancomunidad] VLAN para los usuarios de la Mancomunidad	[3]	[3]	[10]	[7]	[7]	[1]	[1]

Tabla 9: AR - Valoración Activos Red

capa: [P] Personal

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[P.ui.Oper] Usuarios Operadores del Sistema	[7]	[7]	[7]	[7]	[7]	[9]	[1]
[P.prov.Oper] Usuarios Proveedores Operadores del Sistema	[7]	[7]	[7]	[7]	[10]	[5]	[1]
[P.prov.Admins] Usuarios Proveedores Administradores del Sistema	[10]	[10]	[10]	[10]	[10]	[5]	[1]
[P.adm.Admins] Usuarios Administradores del Sistema	[10]	[10]	[10]	[10]	[10]	[9]	[1]
[P.ui.UsuInternos] Usuarios Internos	[4]	[5]	[5]	[5]	[7]	[5]	[1]
[P.ue.Oposicion] Usuarios miembros de la Oposición Política	[0]	[3]	[3]	[10]	[7]	[1]	[1]
[P.ue.Mancomunidad] Usuarios de la Mancomunidad	[0]	[5]	[5]	[5]	[7]	[1]	[1]

Tabla 10: AR - Valoración Activos Personal

capa: [D] Datos

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[D.conf.Virtualización] BD de los vCenters	[7]	[7]	[5]	[7]	[7]	[7]	

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[D.files.PerfilesVDI] Datos de los Escritorios de VDI	[9]	[9]	[10]	[10]	[10]	[9]	[1]
[D.conf.PlantillasVDI] Plantillas VDI	[3]	[7]	[2]	[2]	[2]	[7]	
[D.logs.VDI] Logs de los vCenters y Horizon	[1]	[6]	[4]	[4]	[7]	[3]	
[D.files.ServFicheros] Datos en Unidades de Red Compartidas	[9]	[9]	[10]	[10]	[10]	[9]	[1]
[D.backup.Respaldos] Datos de las copias de Seguridad	[8]	[9]	[10]	[10]	[10]	[9]	[1]
[D.files.BD_Contabilidad] BD Aplicación Contabilidad	[8]	[9]	[10]	[10]	[10]	[9]	[1]
[D.files.BD_Recaudacion] BD Aplicación Recaudación	[8]	[9]	[10]	[10]	[10]	[9]	[1]
[D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos	[3]	[5]	[7]	[7]	[7]	[5]	[1]
[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo	[4]	[6]	[10]	[10]	[10]	[5]	[1]
[D.files.BD_GIS] BD Aplicación GIS	[7]	[7]	[7]	[7]	[7]	[7]	[1]
[D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware	[2]	[5]	[7]	[5]	[7]	[1]	[1]
[D.files.BD_Padron] BD Aplicación WPadron	[8]	[10]	[10]	[10]	[10]	[9]	[1]
[D.files.BD_Nominas] BD Aplicación A3Nom	[6]	[9]	[10]	[10]	[10]	[9]	[1]
[D.conf.GPO] Datos de configuración de las GPOs	[5]	[7]	[2]	[7]	[10]	[5]	
[D.files.BD_Eurocop] BD Aplicación Eurocop	[6]	[9]	[10]	[10]	[10]	[9]	[1]
[D.logs.Windows] Logs de Windows	[0]	[6]	[2]	[2]	[7]	[3]	

Tabla 11: AR - Valoración Activos Datos

4.1.4. Análisis de Amenazas

Debido a la extensión del apartado se opta por generar un informe automático con la herramienta PILAR donde se documenta para cada activo las amenazas relacionadas, la probabilidad con la que estas pueden suceder (con rango entre 0 y 100) basada en la frecuencia esperada de ocurrencia ARO (Annual Rate of Occurrence) y finalmente el impacto para cada una de las dimensiones de seguridad que hemos valorado en los activos.

Ver producto obtenido del TFM (Análisis de amenazas.pdf)

Tabla 12: AR - Análisis de Amenazas (producto obtenido Análisis de amenazas.pdf)

4.1.5. Impacto Potencial

El impacto potencial nos permite conocer cuales son los activos que después de sufrir degradación debido a una amenaza impactan con más fuerza en el modelo de negocio de nuestra organización. Vamos a calcularlo automáticamente mediante la herramienta PILAR (las casillas en blanco no aplican, se resaltan los contenedores de activos con fondos de celda en gris y los subcontenedores con fondos de celda en azul):

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[L.building_CC] Casa Consistorial	[10]				
[L.building_CP] Centro Polivalente	[3]				
[L.local_CPD] CPD Casa Consistorial	[10]				
[L.building_SP] Satélite Policía	[3]				
[L.ST] Servicios Técnicos	[5]				
[L.building_ST] Servicios Técnicos	[5]				
[L.channel_fibraST] Fibra Servicios Técnicos Casa Consistorial	[5]				
[L.BIBLIO] Biblioteca	[1]				
[L.building_Biblioteca] Biblioteca	[1]				
[L.channel_fibraB] Fibra Biblioteca Casa Consistorial	[1]				

Tabla 13: AR - Impacto Potencial Activos Instalaciones

[SW] Aplicación

activo	[D]	[I]	[C]	[A]	[T]
[SW.Aplicaciones] Servidores de Aplicaciones	[8]	[10]	[10]		
[SW.APP.Padron] WPadron	[8]	[10]	[10]		
[SW.APP.Eurocop] Eurocop Servidor	[6]	[9]	[10]		
[SW.APP.Nominas] A3Nom	[6]	[9]	[10]		
[SW.APP.GLPI] Gestion Informatica GLPI	[3]	[6]	[5]		
[SW.APP.Impresion] Servidor Impresión MyQ	[3]	[3]	[3]		
[SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo	[4]	[6]	[10]		
[SW.www.Intranet] Servicio Intranet Local	[3]	[5]	[10]		
[SW.office] Software Ofimática	[2]	[2]	[2]		
[SW.office.Libre7] LibreOffice7	[2]	[2]	[2]		
[SW.office.Office13ADV] Office 2013 advanced	[2]	[2]	[2]		
[SW.office.Office13STA] Office 2013 standard	[2]	[2]	[2]		
[SW.Clientes] Software Cliente	[7]	[7]	[7]		

activo	[D]	[I]	[C]	[A]	[T]
[SW.Other.Padron] Padrón Cliente	[1]	[1]	[3]		
[SW.Other.Eurocop] Eurocop Cliente	[1]	[1]	[3]		
[SW.Other.Lexnet] Lexnet Cliente	[1]	[1]	[5]		
[SW.Other.Siltra] Siltra Cliente	[1]	[1]	[3]		
[SW.Other.ZKSoft] ZkSoftware Cliente Control Accesos	[1]	[1]	[3]		
[SW.Other.GIS] Software de Gestión Territorial Cliente	[7]	[7]	[7]		
[SW.Other.Reca] ATM Recaudación Cliente	[1]	[1]	[3]		
[SW.Other.VNC] VNC Cliente	[1]	[1]	[3]		
[SW.Other.Conta] ATM Contabilidad Cliente	[1]	[1]	[3]		
[SW.Other.AutoCAD19] Software Autocad 2019	[2]	[2]	[2]		
[SW.Other.Presto] Software Presto 2019	[2]	[2]	[2]		
[SW.Other.SondaProveedor] Sonda Servicio Proveedor Mantenimiento	[2]	[4]	[4]		
[SW.Cloud] Software en Cloud	[8]	[9]	[10]		
[SW.email_server.Postfix] Servidor Correo	[8]	[9]	[10]		
[SW.www.Plesk_1] Servidor Plesk Correo	[8]	[9]	[10]		
[SW.www.Plesk_2] Servidor Plesk Web	[8]	[9]	[5]		
[SW.www.WebAyto] Servicio Wordpress	[8]	[9]	[5]		
[SW.Pruebas] Servidores Pruebas	[0]	[0]	[5]		
[SW.Other.Pruebas_2] Servidor Pruebas	[0]	[0]	[5]		
[SW.Other.Pruebas_3] Servidor Pruebas	[0]	[0]	[5]		
[SW.Other.Pruebas_1] Servidor Pruebas	[0]	[0]	[5]		
[SW.Virtualización] Virtualización de Infraestructura y Escritorios	[10]	[10]	[10]		
[SW.APP.VDIConnection_1] Servidor VDI Connection	[7]	[3]	[3]		
[SW.APP.VDIConnection_3] Servidor VDI Connection	[7]	[3]	[3]		
[SW.APP.VDIConnection_2] Servidor VDI Connection	[7]	[3]	[3]		
[SW.APP.VDIComposer] Servidor VDI Composer	[2]	[3]	[3]		
[SW.APP.VDISecurity] Servidor VDI Security	[7]	[7]	[7]		
[SW.file.PerfilesVDI] Servidor ficheros de Perfiles VDI	[7]	[9]	[10]		
[SW.hypervisor.Horizon7] Horizon VDI	[7]	[7]	[10]		
[SW.hypervisor.vCenterInfra] vCenter Infraestructura	[10]	[10]	[10]		
[SW.hypervisor.vCenterVDI] vCenter VDI	[7]	[7]	[10]		
[SW.infra] Software de Infraestructura	[9]	[9]	[10]		
[SW.directory.DC_1] Controlador Dominio DNS	[7]	[8]	[7]		
[SW.directory.DC_2] Controlador Dominio DNS	[7]	[8]	[7]		
[SW.directory.DHCP_1] Servidor DHCP	[7]	[3]	[3]		

activo	[D]	[I]	[C]	[A]	[T]
[SW.directory.DHCP_2] Servidor DHCP	[7]	[3]	[3]		
[SW.APP.KMS] Servidor Licencias Microsoft	[2]	[3]	[5]		
[SW.APP.WSUS] Servidor Actualizaciones Microsoft	[2]	[2]	[2]		
[SW.file.Ficheros] Servidor de Ficheros	[9]	[9]	[10]		
[SW.Other.Santricity] Gestor de Storage	[0]	[0]	[0]		
[SW.backup] Software de Backup	[8]	[9]	[10]		
[SW.backup.Backup_1] Servidor VDP Backup	[8]	[9]	[10]		
[SW.backup.Backup_2] Servidor VDP Backup	[8]	[9]	[10]		
[SW.dbms.SQL12] Servidor SQL Server 2012	[10]	[10]	[10]		
[SW.seguridad] Software de seguridad	[8]	[8]	[8]		
[SW.AV.SophosServer] Sophos Advanced Server	[8]	[8]	[8]		
[SW.AV.SophosFisicos] Sophos Standard Equipos Físicos	[6]	[6]	[6]		
[SW.AV.SophosVDI] Sophos Advanced VDI	[6]	[6]	[6]		
[SW.APP.ServerEndpoint_2] Servidor Sophos Endpoint	[8]	[8]	[8]		
[SW.APP.ServerEndpoint_1] Servidor Sophos Endpoint	[8]	[8]	[8]		
[SW.OS.WIN12] Server 2012 R2	[10]	[10]	[10]		
[SW.OS.WIN16] Server 2016 VDI	[2]	[2]	[2]		
[SW.OS.WIN10] Windows 10	[2]	[2]	[2]		
[SW.OS.CENT7] Server Linux Centos 7	[8]	[9]	[10]		

Tabla 14: AR - Impacto Potencial Activos Aplicación

[S] Servicios

activo	[D]	[I]	[C]	[A]	[T]
[S.cloud.SophosCentral] Central Endpoint Cloud de Sophos	[7]	[8]	[8]	[10]	[10]
[S.other.Mantenimiento] Mantenimiento para el CPD	[6]	[10]	[10]	[10]	[10]
[S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes	[9]	[10]	[10]	[10]	[10]
[S.iaas.MailWeb] Proveedor de Infraestructura como Servicio	[8]	[9]	[10]	[10]	[10]
[S.ca.Certs] Proveedor de certificados FNMT	[5]	[6]	[6]	[10]	[6]
[S.other.Soporte] Proveedores de soporte de aplicaciones	[3]	[7]	[7]	[7]	[10]
[S.isp.Internet] Proveedor de acceso a Internet	[10]	[9]	[10]	[10]	[10]

Tabla 15: AR - Impacto Potencial Activos Servicios

[AUX] Equipamiento Auxiliar

activo	[D]	[I]	[C]	[A]	[T]
[AUX.CPD] elementos del CPD	[8]	[2]	[7]		
[AUX.ups.CPD_2] UPS del CPD	[4]				
[AUX.ac.CPD_2] Split de Aire Acondicionado del CPD	[7]				
[AUX.furniture.RackCPD_2] Rack CPD	[7]	[0]	[0]		
[AUX.furniture.RackCPD_1] Rack CPD	[7]	[0]	[0]		
[AUX.furniture.Armario] Armario Ignífugo Caja Fuerte	[0]	[0]	[7]		
[AUX.ac.CPD_1] Split de Aire Acondicionado del CPD	[7]				
[AUX.ups.CPD_1] UPS del CPD	[4]				
[AUX.other.Extintor] Extintor de CO2	[0]	[0]	[0]		
[AUX.other.AccesoCPD] Sistema de control de acceso con alarma al CPD	[8]	[2]	[7]		
[AUX.ups.SatPolicia] Mini UPS del Satélite de Policía	[0]				
[AUX.ups.CentroPol] Mini UPS del Centro Polivalente	[0]				

Tabla 16: AR - Impacto Potencial Activos Equipamiento Auxiliar

[HW] Hardware

activo	[D]	[I]	[C]	[A]	[T]
[HW.CPD] Equipos del CPD	[10]	[10]	[10]		
[HW.CPD.INFRA] HW Virtualización Equipos Infraestructura	[10]	[10]	[10]		
[HW.host.INFRA_2] ESX Infraestructura	[10]	[7]	[10]		
[HW.host.INFRA_1] ESX Infraestructura	[10]	[7]	[10]		
[HW.data.CabinaProd] Cabina de Producción	[10]	[10]	[10]		
[HW.vhost.Switch] Switch Virtual Servidores Infraestructura	[10]	[1]	[3]		
[HW.data.DataStores_3] DataStores Virtuales Equipos Infraestructura	[10]	[10]	[10]		
[HW.data.DataStores_2] DataStores Virtuales Backup	[9]	[9]	[10]		
[HW.data.CabinaBack] Cabina de Backup	[9]	[9]	[10]		
[HW.vhost.Servidores] Máquinas Virtuales Servidores Infraestructura	[10]	[7]	[9]		
[HW.CPD.VDI] Hardware Virtualización de Escritorios	[7]	[7]	[10]		
[HW.host.VDI_2] ESX VDI	[6]	[2]	[5]		
[HW.host.VDI_3] ESX VDI	[6]	[2]	[5]		
[HW.host.VDI_1] ESX VDI	[6]	[2]	[5]		
[HW.data.DataStores_1] DataStores Virtuales Escritorios	[7]	[7]	[10]		

activo	[D]	[I]	[C]	[A]	[T]
Usuarios vSAN					
[HW.vhost.Switch_1] Switch Virtual Escritorios Usuarios	[7]	[1]	[3]		
[HW.vhost.VDI] Máquinas Virtuales Escritorios Usuarios	[2]	[0]	[6]		
[HW.CPD.COM] Comunicaciones CPD	[10]	[7]	[9]		
[HW.other.Firewall_2] Firewall en HA	[9]	[6]	[9]		
[HW.other.Firewall_1] Firewall en HA	[9]	[6]	[9]		
[HW.Other.SwitchStack] Core Switch Stack 10G	[10]	[7]	[9]		
[HW.switch.SwitchCPD_2] Switch de Usuario CPD	[6]	[1]	[3]		
[HW.switch.SwitchCPD_1] Switch de Usuario CPD	[6]	[1]	[3]		
[HW.router.CPD_2] Router ADSL Servicio Correo Postal	[2]	[1]	[6]		
[HW.router.CPD_3] Router ADSL Red SARA	[4]	[4]	[9]		
[HW.router.CPD_1] Router Fibra Principal CPD	[9]	[4]	[6]		
[HW.CentroPol] Equipos Centro Polivalente	[3]	[6]	[8]		
[HW.other.MiniFW_2] Firewall Centro Polivalente	[3]	[6]	[8]		
[HW.router.CentroPol] Router Fibra Centro Polivalente	[3]	[6]	[8]		
[HW.switch.SwitchST] Switch de Usuario Servicios Técnicos	[6]	[1]	[3]		
[HW.SatPolicia] Equipos Satélite Policía	[3]	[6]	[8]		
[HW.router.SatPolicia] Router Fibra Satélite Policía	[3]	[6]	[8]		
[HW.other.MiniFW_1] Firewall Satélite Policía	[3]	[6]	[8]		
[HW.switch.SwitchCCP2] Switch de Usuario Casa Consistorial P2	[6]	[1]	[3]		
[HW.switch.SwitchBiblio] Switch de Usuario Biblioteca	[3]	[1]	[3]		
[HW.pc.ZeroClient] Equipos de Usuarios Virtualizados	[2]	[0]	[6]		
[HW.pc.Equipo] Equipos de Usuarios	[2]	[0]	[4]		
[HW.mobile.PortatilTeletrabajo] Equipo Portátil para Teletrabajo	[2]	[0]	[6]		
[HW.print.Impresoras] Impresoras	[5]	[0]	[4]		
[HW.vhost.Cloud] Máquinas Virtuales Servidores Infraestructura Cloud	[8]	[6]	[9]		

Tabla 17: AR - Impacto Potencial Activos Hardware

[COM] Red

activo	[D]	[I]	[C]	[A]	[T]
[COM.CentroPol] Comunicaciones Centro Polivalente	[2]	[7]	[8]	[9]	
[COM.other.CentroPol] Túnel Centro Polivalente CPD	[2]	[7]	[8]	[9]	
[COM.wan.CentroPol] WAN del Centro Polivalente	[2]	[7]	[8]	[9]	
[COM.SatPolicia] Comunicaciones Satélite Policía	[2]	[7]	[8]	[9]	

activo	[D]	[I]	[C]	[A]	[T]
[COM.other.SatPolicia] Túnel Satélite Policía CPD	[2]	[7]	[8]	[9]	
[COM.wan.SatPolicia] WAN del Satélite Policía	[2]	[7]	[8]	[9]	
[COM.CPD] Comunicaciones CPD	[9]	[8]	[9]	[10]	
[COM.vpn.RedSara] VPN con la Red Sara	[3]	[5]	[9]	[10]	
[COM.other.Teletrabajo] Conexión contra servidor de seguridad PCoIP	[6]	[5]	[6]	[10]	
[COM.vpn.RedMonitor] VPN con la Red de Monitorización para mantenimiento	[1]	[2]	[3]	[4]	
[COM.adsl.CPD_2] ADSL Correos Postal IP fija	[1]	[2]	[6]	[2]	
[COM.wan.CPD] WAN del CPD	[8]	[5]	[6]	[10]	
[COM.vlan.ILO] VLAN para las ilos de los hosts	[1]	[2]	[1]	[7]	
[COM.vlan.VSAN] VLAN para el servicio de vSAN	[5]	[2]	[1]	[4]	
[COM.adsl.CPD_1] ADSL Red Sara IP fija	[3]	[5]	[9]	[10]	
[COM.vlan.EquiposInfra] VLAN para los Equipos de Infraestructura	[9]	[8]	[9]	[10]	
[COM.vlan.EquiposUsuario] VLAN para los usuarios de Usuario Interno	[8]	[7]	[8]	[7]	
[COM.vlan.EquiposMancomunidad] VLAN para los usuarios de la Mancomunidad	[2]	[1]	[9]	[7]	

Tabla 18: AR - Impacto Potencial Activos Red

[P] Personal

activo	[D]	[I]	[C]	[A]	[T]
[P.ui.Oper] Usuarios Operadores del Sistema	[6]	[6]	[5]		
[P.prov] Usuarios Proveedores	[7]	[9]	[9]		
[P.prov.Oper] Usuarios Proveedores Operadores del Sistema	[4]	[6]	[6]		
[P.prov.Admins] Usuarios Proveedores Administradores del Sistema	[7]	[9]	[9]		
[P.adm.Admins] Usuarios Administradores del Sistema	[9]	[10]	[10]		
[P.ui.UsuInternos] Usuarios Internos	[3]	[4]	[3]		
[P.ue.Oposicion] Usuarios miembros de la Oposición Política	[0]	[2]	[0]		
[P.ue.Mancomunidad] Usuarios de la Mancomunidad	[0]	[4]	[2]		

Tabla 19: AR - Impacto Potencial Activos Personal

[D] Datos

activo	[D]	[I]	[C]	[A]	[T]
[D.Virtualizacion] Datos relacionados con la Virtualización	[6]	[6]	[9]	[10]	

activo	[D]	[I]	[C]	[A]	[T]
[D.conf.Virtualización] BD de los vCenters	[4]	[4]	[4]	[7]	
[D.files.PerfilesVDI] Datos de los Escritorios de VDI	[6]	[6]	[9]	[10]	
[D.conf.PlantillasVDI] Plantillas VDI	[0]	[4]	[1]	[2]	
[D.logs.VDI] Logs de los vCenters y Horizon	[0]	[5]	[3]	[4]	
[D.files.ServFicheros] Datos en Unidades de Red Compartidas	[3]	[6]	[9]	[10]	
[D.backup.Respaldos] Datos de las copias de Seguridad	[2]	[6]	[9]	[10]	
[D.BDSQLServer] BD contenidas en el servidor de SQL	[2]	[6]	[9]	[10]	
[D.files.BD_Contabilidad] BD Aplicación Contabilidad	[2]	[6]	[9]	[10]	
[D.files.BD_Recaudacion] BD Aplicación Recaudación	[2]	[6]	[9]	[10]	
[D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos	[0]	[2]	[6]	[7]	
[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo	[0]	[3]	[9]	[10]	
[D.files.BD_GIS] BD Aplicación GIS	[1]	[4]	[6]	[7]	
[D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware	[0]	[2]	[6]	[5]	
[D.files.BD_Padron] BD Aplicación WPadron	[2]	[7]	[9]	[10]	
[D.files.BD_Nominas] BD Aplicación A3Nom	[0]	[6]	[9]	[10]	
[D.conf.GPO] Datos de configuración de las GPOs	[2]	[4]	[1]	[7]	
[D.files.BD_Eurocop] BD Aplicación Eurocop	[0]	[6]	[9]	[10]	
[D.logs.Windows] Logs de Windows	[0]	[5]	[1]	[2]	

Tabla 20: AR - Impacto Potencial Activos Datos

4.1.6. Nivel de riesgo

Una vez conocido el impacto pasaremos a calcular el riesgo aplicándole la frecuencia, de este modo podremos priorizar nuestro plan de mejora. En cuanto a los niveles de criticidad, MAGERIT los calcula del siguiente modo:

- {0} := despreciable
- {1} := bajo
- {2} := medio
- {3} := alto
- {4} := muy alto
- {5} := crítico
- {6} := muy crítico
- {7} := extremadamente crítico
- {8} := desastre
- {9} := catástrofe

Nuevamente realizamos los cálculos de modo automatizado con la herramienta PILAR:

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[L.building_CC] Casa Consistorial	{6,8}	-	-	-	-
[L.building_CP] Centro Polivalente	{2,7}	-	-	-	-
[L.local_CPD] CPD Casa Consistorial	{6,8}	-	-	-	-
[L.building_SP] Satélite Policía	{2,7}	-	-	-	-
[L.ST] Servicios Técnicos	{3,9}	-	-	-	-
[L.building_ST] Servicios Técnicos	{3,9}	-	-	-	-
[L.channel_fibraST] Fibra Servicios Técnicos Casa Consistorial	{3,9}	-	-	-	-
[L.BIBLIO] Biblioteca	{1,5}	-	-	-	-
[L.building_Biblioteca] Biblioteca	{1,5}	-	-	-	-
[L.channel_fibraB] Fibra Biblioteca Casa Consistorial	{1,5}	-	-	-	-

Tabla 21: AR - Nivel de riesgo Activos Instalaciones

[SW] Aplicación

activo	[D]	[I]	[C]	[A]	[T]
[SW.Aplicaciones] Servidores de Aplicaciones	{5,7}	{6,8}	{6,8}	-	-
[SW.APP.Padron] WPadron	{5,7}	{6,8}	{6,8}	-	-
[SW.APP.Eurocop] Eurocop Servidor	{4,5}	{6,2}	{6,8}	-	-
[SW.APP.Nominas] A3Nom	{4,5}	{6,2}	{6,8}	-	-
[SW.APP.GLPI] Gestion Informática GLPI	{2,7}	{4,5}	{3,9}	-	-
[SW.APP.Impresion] Servidor Impresión MyQ	{2,7}	{2,7}	{2,7}	-	-
[SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo	{3,3}	{4,5}	{6,8}	-	-
[SW.www.Intranet] Servicio Intranet Local	{2,7}	{3,9}	{6,8}	-	-
[SW.office] Software Ofimática	{2,1}	{2,1}	{2,1}	-	-
[SW.office.Libre7] LibreOffice7	{2,1}	{2,1}	{2,1}	-	-
[SW.office.Office13ADV] Office 2013 advanced	{2,1}	{2,1}	{2,1}	-	-
[SW.office.Office13STA] Office 2013 standard	{2,1}	{2,1}	{2,1}	-	-
[SW.Clientes] Software Cliente	{5,1}	{5,1}	{5,1}	-	-
[SW.Other.Padron] Padrón Cliente	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.Eurocop] Eurocop Cliente	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.Lexnet] Lexnet Cliente	{1,5}	{1,5}	{3,9}	-	-
[SW.Other.Siltra] Siltra Cliente	{1,5}	{1,5}	{2,7}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[SW.Other.ZKSoft] ZkSoftware Cliente Control Accesos	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.GIS] Software de Gestión Territorial Cliente	{5,1}	{5,1}	{5,1}	-	-
[SW.Other.Reca] ATM Recaudación Cliente	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.VNC] VNC Cliente	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.Conta] ATM Contabilidad Cliente	{1,5}	{1,5}	{2,7}	-	-
[SW.Other.AutoCAD19] Software Autocad 2019	{2,1}	{2,1}	{2,1}	-	-
[SW.Other.Presto] Software Presto 2019	{2,1}	{2,1}	{2,1}	-	-
[SW.Other.SondaProveedor] Sonda Servicio Proveedor Mantenimiento	{2,1}	{3,3}	{3,3}	-	-
[SW.Cloud] Software en Cloud	{5,7}	{6,2}	{6,8}	-	-
[SW.email_server.Postfix] Servidor Correo	{5,7}	{6,2}	{6,8}	-	-
[SW.www.Plesk_1] Servidor Plesk Correo	{5,7}	{6,2}	{6,8}	-	-
[SW.www.Plesk_2] Servidor Plesk Web	{5,7}	{6,2}	{3,9}	-	-
[SW.www.WebAyto] Servicio Wordpress	{5,7}	{6,2}	{3,9}	-	-
[SW.Pruebas] Servidores Pruebas	{0,98}	{0,98}	{3,9}	-	-
[SW.Other.Pruebas_2] Servidor Pruebas	{0,98}	{0,98}	{3,9}	-	-
[SW.Other.Pruebas_3] Servidor Pruebas	{0,98}	{0,98}	{3,9}	-	-
[SW.Other.Pruebas_1] Servidor Pruebas	{0,98}	{0,98}	{3,9}	-	-
[SW.Virtualización] Virtualización de Infraestructura y Escritorios	{6,8}	{6,8}	{6,8}	-	-
[SW.APP.VDIConnection_1] Servidor VDI Connection	{5,1}	{2,7}	{2,7}	-	-
[SW.APP.VDIConnection_3] Servidor VDI Connection	{5,1}	{2,7}	{2,7}	-	-
[SW.APP.VDIConnection_2] Servidor VDI Connection	{5,1}	{2,7}	{2,7}	-	-
[SW.APP.VDIComposer] Servidor VDI Composer	{2,1}	{2,7}	{2,7}	-	-
[SW.APP.VDISecurity] Servidor VDI Security	{5,1}	{5,1}	{5,1}	-	-
[SW.file.PerfilesVDI] Servidor ficheros de Perfiles VDI	{5,1}	{6,2}	{6,8}	-	-
[SW.hypervisor.Horizon7] Horizon VDI	{5,1}	{5,1}	{6,8}	-	-
[SW.hypervisor.vCenterInfra] vCenter Infraestructura	{6,8}	{6,8}	{6,8}	-	-
[SW.hypervisor.vCenterVDI] vCenter VDI	{5,1}	{5,1}	{6,8}	-	-
[SW.infra] Software de Infraestructura	{6,2}	{6,2}	{6,8}	-	-
[SW.directory.DC_1] Controlador Dominio DNS	{5,1}	{5,7}	{5,1}	-	-
[SW.directory.DC_2] Controlador Dominio DNS	{5,1}	{5,7}	{5,1}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[SW.directory.DHCP_1] Servidor DHCP	{5,1}	{2,7}	{2,7}	-	-
[SW.directory.DHCP_2] Servidor DHCP	{5,1}	{2,7}	{2,7}	-	-
[SW.APP.KMS] Servidor Licencias Microsoft	{2,1}	{2,7}	{3,9}	-	-
[SW.APP.WSUS] Servidor Actualizaciones Microsoft	{2,1}	{2,1}	{2,1}	-	-
[SW.file.Ficheros] Servidor de Ficheros	{6,2}	{6,2}	{6,8}	-	-
[SW.Other.Santricity] Gestor de Storage	{0,98}	{0,98}	{0,98}	-	-
[SW.backup] Software de Backup	{5,7}	{6,2}	{6,8}	-	-
[SW.backup.Backup_1] Servidor VDP Backup	{5,7}	{6,2}	{6,8}	-	-
[SW.backup.Backup_2] Servidor VDP Backup	{5,7}	{6,2}	{6,8}	-	-
[SW.dbms.SQL12] Servidor SQL Server 2012	{6,8}	{6,8}	{6,8}	-	-
[SW.seguridad] Software de seguridad	{5,7}	{5,7}	{5,7}	-	-
[SW.AV.SophosServer] Sophos Advanced Server	{5,7}	{5,7}	{5,7}	-	-
[SW.AV.SophosFisicos] Sophos Standard Equipos Físicos	{4,5}	{4,5}	{4,5}	-	-
[SW.AV.SophosVDI] Sophos Advanced VDI	{4,5}	{4,5}	{4,5}	-	-
[SW.APP.ServerEndpoint_2] Servidor Sophos Endpoint	{5,7}	{5,7}	{5,7}	-	-
[SW.APP.ServerEndpoint_1] Servidor Sophos Endpoint	{5,7}	{5,7}	{5,7}	-	-
[SW.OS.WIN12] Server 2012 R2	{6,8}	{6,8}	{6,8}	-	-
[SW.OS.WIN16] Server 2016 VDI	{2,1}	{2,1}	{2,1}	-	-
[SW.OS.WIN10] Windows 10	{2,1}	{2,1}	{2,1}	-	-
[SW.OS.CENT7] Server Linux Centos 7	{5,7}	{6,2}	{6,8}	-	-

Tabla 22: AR - Nivel de riesgo Activos Aplicación

[S] Servicios

activo	[D]	[I]	[C]	[A]	[T]
[S.cloud.SophosCentral] Central Endpoint Cloud de Sophos	{5,1}	{5,1}	{5,1}	{6,2}	{6,8}
[S.other.Mantenimiento] Mantenimiento para el CPD	{4,5}	{6,3}	{6,3}	{6,2}	{6,8}
[S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes	{6,3}	{6,3}	{6,3}	{6,2}	{6,8}
[S.iaas.MailWeb] Proveedor de Infraestructura como Servicio	{5,7}	{5,7}	{6,3}	{6,2}	{6,8}
[S.ca.Certs] Proveedor de certificados FNMT	{3,9}	{3,9}	{3,9}	{6,2}	{4,5}
[S.other.Soporte] Proveedores de soporte de aplicaciones	{2,8}	{4,5}	{4,5}	{4,5}	{6,8}

activo	[D]	[I]	[C]	[A]	[T]
[S.isp.Internet] Proveedor de acceso a Internet	{6,8}	{5,7}	{6,3}	{6,2}	{6,8}

Tabla 23: AR - Nivel de riesgo Activos Servicios

[AUX] Equipamiento Auxiliar

activo	[D]	[I]	[C]	[A]	[T]
[AUX.CPD] elementos del CPD	{5,4}	{2,1}	{5,1}	-	-
[AUX.ups.CPD_2] UPS del CPD	{3,3}	-	-	-	-
[AUX.ac.CPD_2] Split de Aire Acondicionado del CPD	{5,1}	-	-	-	-
[AUX.furniture.RackCPD_2] Rack CPD	{4,8}	{0,28}	{0,88}	-	-
[AUX.furniture.RackCPD_1] Rack CPD	{4,8}	{0,28}	{0,88}	-	-
[AUX.furniture.Armario] Armario Ignífugo Caja Fuerte	{0,93}	{0,63}	{5,1}	-	-
[AUX.ac.CPD_1] Split de Aire Acondicionado del CPD	{5,1}	-	-	-	-
[AUX.ups.CPD_1] UPS del CPD	{3,3}	-	-	-	-
[AUX.other.Extintor] Extintor de CO2	{0,93}	{0,28}	{0,88}	-	-
[AUX.other.AccesoCPD] Sistema de control de acceso con alarma al CPD	{5,4}	{2,1}	{5,1}	-	-
[AUX.ups.SatPolicia] Mini UPS del Satélite de Policía	{0,63}	-	-	-	-
[AUX.ups.CentroPol] Mini UPS del Centro Polivalente	{0,63}	-	-	-	-

Tabla 24: AR - Nivel de riesgo Activos Equipamiento Auxiliar

[HW] Hardware

activo	[D]	[I]	[C]	[A]	[T]
[HW.CPD] Equipos del CPD	{7,2}	{6,8}	{6,8}	-	-
[HW.CPD.INFRA] HW Virtualización Equipos Infraestructura	{7,2}	{6,8}	{6,8}	-	-
[HW.host.INFRA_2] ESX Infraestructura	{7,2}	{5,1}	{6,3}	-	-
[HW.host.INFRA_1] ESX Infraestructura	{7,2}	{5,1}	{6,3}	-	-
[HW.data.CabinaProd] Cabina de Producción	{7,2}	{6,8}	{6,8}	-	-
[HW.vhost.Switch] Switch Virtual Servidores Infraestructura	{7,2}	{1,5}	{2,8}	-	-
[HW.data.DataStores_3] DataStores Virtuales Equipos Infraestructura	{7,2}	{6,8}	{6,8}	-	-
[HW.data.DataStores_2] DataStores Virtuales	{6,6}	{6,2}	{6,8}	-	-

activo	[D]	[I]	[C]	[A]	[T]
Backup					
[HW.data.CabinaBack] Cabina de Backup	{6,6}	{6,2}	{6,8}	-	-
[HW.vhost.Servidores] Máquinas Virtuales Servidores Infraestructura	{7,2}	{5,1}	{6,3}	-	-
[HW.CPD.VDI] Hardware Virtualización de Escritorios	{5,4}	{5,1}	{6,8}	-	-
[HW.host.VDI_2] ESX VDI	{4,8}	{2,1}	{3,4}	-	-
[HW.host.VDI_3] ESX VDI	{4,8}	{2,1}	{3,4}	-	-
[HW.host.VDI_1] ESX VDI	{4,8}	{2,1}	{3,4}	-	-
[HW.data.DataStores_1] DataStores Virtuales Escritorios Usuarios vSAN	{5,4}	{5,1}	{6,8}	-	-
[HW.vhost.Switch_1] Switch Virtual Escritorios Usuarios	{5,4}	{1,5}	{2,8}	-	-
[HW.vhost.VDI] Máquinas Virtuales Escritorios Usuarios	{2,5}	{0,87}	{4,5}	-	-
[HW.CPD.COM] Comunicaciones CPD	{7,2}	{5,1}	{6,3}	-	-
[HW.other.Firewall_2] Firewall en HA	{6,6}	{4,5}	{6,3}	-	-
[HW.other.Firewall_1] Firewall en HA	{6,6}	{4,5}	{6,3}	-	-
[HW.Other.SwitchStack] Core Switch Stack 10G	{7,2}	{5,1}	{6,3}	-	-
[HW.switch.SwitchCPD_2] Switch de Usuario CPD	{4,8}	{1,5}	{2,8}	-	-
[HW.switch.SwitchCPD_1] Switch de Usuario CPD	{4,8}	{1,5}	{2,8}	-	-
[HW.router.CPD_2] Router ADSL Servicio Correo Postal	{2,5}	{1,5}	{4,5}	-	-
[HW.router.CPD_3] Router ADSL Red SARA	{3,7}	{3,3}	{6,3}	-	-
[HW.router.CPD_1] Router Fibra Principal CPD	{6,6}	{3,3}	{4,5}	-	-
[HW.CentroPol] Equipos Centro Polivalente	{3,1}	{4,5}	{5,7}	-	-
[HW.other.MiniFW_2] Firewall Centro Polivalente	{3,1}	{4,5}	{5,7}	-	-
[HW.router.CentroPol] Router Fibra Centro Polivalente	{3,1}	{4,5}	{5,7}	-	-
[HW.switch.SwitchST] Switch de Usuario Servicios Técnicos	{4,8}	{1,5}	{2,8}	-	-
[HW.SatPolicia] Equipos Satélite Policía	{3,1}	{4,5}	{5,7}	-	-
[HW.router.SatPolicia] Router Fibra Satélite Policiía	{3,1}	{4,5}	{5,7}	-	-
[HW.other.MiniFW_1] Firewall Satélite Policía	{3,1}	{4,5}	{5,7}	-	-
[HW.switch.SwitchCCP2] Switch de Usuario Casa Consistorial P2	{4,8}	{1,5}	{2,8}	-	-
[HW.switch.SwitchBiblio] Switch de Usuario Biblioteca	{3,1}	{1,5}	{2,8}	-	-
[HW.pc.ZeroClient] Equipos de Usuarios Virtualizados	{2,5}	{0,87}	{4,5}	-	-
[HW.pc.Equipo] Equipos de Usuarios	{2,5}	{0,87}	{3,4}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[HW.mobile.PortatilTeletrabajo] Equipo Portátil para Teletrabajo	{2,5}	{0,87}	{4,5}	-	-
[HW.print.Impresoras] Impresoras	{4,2}	{0,87}	{3,4}	-	-
[HW.vhost.Cloud] Máquinas Virtuales Servidores Infraestructura Cloud	{6,0}	{4,5}	{6,3}	-	-

Tabla 25: AR - Nivel de riesgo Activos Hardware

[COM] Red

activo	[D]	[I]	[C]	[A]	[T]
[COM.CentroPol] Comunicaciones Centro Polivalente	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.other.CentroPol] Túnel Centro Polivalente CPD	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.wan.CentroPol] WAN del Centro Polivalente	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.SatPolicia] Comunicaciones Satélite Policía	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.other.SatPolicia] Túnel Satélite Policía CPD	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.wan.SatPolicia] WAN del Satélite Policía	{3,1}	{5,0}	{5,7}	{6,2}	-
[COM.CPD] Comunicaciones CPD	{7,2}	{5,6}	{6,3}	{6,8}	-
[COM.vpn.RedSara] VPN con la Red Sara	{3,7}	{3,8}	{6,3}	{6,8}	-
[COM.other.Teletrabajo] Conexión contra servidor de seguridad PCoIP	{5,4}	{3,8}	{4,5}	{6,8}	-
[COM.vpn.RedMonitor] VPN con la Red de Monitorización para mantenimiento	{2,5}	{2,1}	{2,8}	{3,3}	-
[COM.adsl.CPD_2] ADSL Correos Postal IP fija	{2,5}	{2,1}	{4,5}	{2,1}	-
[COM.wan.CPD] WAN del CPD	{6,6}	{3,8}	{4,5}	{6,8}	-
[COM.vlan.ILO] VLAN para las ilos de los hosts	{2,5}	{2,1}	{1,6}	{5,1}	-
[COM.vlan.VSAN] VLAN para el servicio de vSAN	{4,8}	{2,1}	{1,6}	{3,3}	-
[COM.adsl.CPD_1] ADSL Red Sara IP fija	{3,7}	{3,8}	{6,3}	{6,8}	-
[COM.vlan.EquiposInfra] VLAN para los Equipos de Infraestructura	{7,2}	{5,6}	{6,3}	{6,8}	-
[COM.vlan.EquiposUsuario] VLAN para los usuarios de Usuario Interno	{6,6}	{5,0}	{5,7}	{5,1}	-
[COM.vlan.EquiposMancomunidad] VLAN para los usuarios de la Mancomunidad	{3,1}	{1,5}	{6,3}	{5,1}	-

Tabla 26: AR - Nivel de riesgo Activos Red

[P] Personal

activo	[D]	[I]	[C]	[A]	[T]
[P.ui.Oper] Usuarios Operadores del Sistema	{4,3}	{4,5}	{4,7}	-	-
[P.prov] Usuarios Proveedores	{5,1}	{6,3}	{6,3}	-	-
[P.prov.Oper] Usuarios Proveedores Operadores del Sistema	{3,3}	{4,5}	{4,5}	-	-
[P.prov.Admins] Usuarios Proveedores Administradores del Sistema	{5,1}	{6,3}	{6,3}	-	-
[P.adm.Admins] Usuarios Administradores del Sistema	{6,3}	{6,8}	{7,2}	-	-
[P.ui.UsuInternos] Usuarios Internos	{2,5}	{3,4}	{3,5}	-	-
[P.ue.Oposicion] Usuarios miembros de la Oposición Política	{0,63}	{2,2}	{1,6}	-	-
[P.ue.Mancomunidad] Usuarios de la Mancomunidad	{0,63}	{3,4}	{2,7}	-	-

Tabla 27: AR - Nivel de riesgo Activos Personal

[D] Datos

activo	[D]	[I]	[C]	[A]	[T]
[D.Virtualizacion] Datos relacionados con la Virtualización	{5,4}	{6,2}	{8,1}	{7,7}	-
[D.conf.Virtualización] BD de los vCenters	{4,2}	{4,2}	{4,2}	{5,9}	-
[D.files.PerfilesVDI] Datos de los Escritorios de VDI	{5,4}	{6,2}	{8,1}	{7,7}	-
[D.conf.PlantillasVDI] Plantillas VDI	{1,8}	{4,2}	{2,5}	{3,0}	-
[D.logs.VDI] Logs de los vCenters y Horizon	{0,93}	{5,7}	{4,5}	{4,2}	-
[D.files.ServFicheros] Datos en Unidades de Red Compartidas	{3,6}	{6,2}	{8,1}	{7,7}	-
[D.backup.Respaldos] Datos de las copias de Seguridad	{3,0}	{6,2}	{8,1}	{7,7}	-
[D.BDSQLServer] BD contenidas en el servidor de SQL	{3,0}	{6,2}	{8,1}	{7,7}	-
[D.files.BD_Contabilidad] BD Aplicación Contabilidad	{3,0}	{6,2}	{8,1}	{7,7}	-
[D.files.BD_Recaudacion] BD Aplicación Recaudación	{3,0}	{6,2}	{8,1}	{7,7}	-
[D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos	{0,81}	{3,9}	{6,3}	{5,9}	-
[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo	{0,93}	{4,5}	{8,1}	{7,7}	-
[D.files.BD_GIS] BD Aplicación GIS	{2,4}	{5,1}	{6,3}	{5,9}	-
[D.acl.BD_ZKSoft] BD Control de Accesos	{0,69}	{3,9}	{6,3}	{4,8}	-

activo	[D]	[I]	[C]	[A]	[T]
Zksoftware					
[D.files.BD_Padron] BD Aplicación WPadron	{3,0}	{6,8}	{8,1}	{7,7}	-
[D.files.BD_Nominas] BD Aplicación A3Nom	{1,8}	{6,2}	{8,1}	{7,7}	-
[D.conf.GPO] Datos de configuración de las GPOs	{3,0}	{4,2}	{2,5}	{5,9}	-
[D.files.BD_Eurocop] BD Aplicación Eurocop	{1,8}	{6,2}	{8,1}	{7,7}	-
[D.logs.Windows] Logs de Windows	{0,46}	{5,7}	{3,4}	{3,0}	-

Tabla 28: AR - Nivel de riesgo Activos Datos

4.1.6.1. Riesgo Aceptable y Riesgo Residual

En el Procedimiento de Revisión por Dirección se lleva como punto de la reunión el Análisis de Riesgos (se facilita el Informe de Análisis de Riesgos con antelación) y la aprobación tanto del Riesgo Aceptable como del Riesgo Residual. Una vez estudiado el análisis de riesgos por la gerencia se establece el nivel “Medio” dentro de los niveles de criticidad del punto 4.2.6. como nivel de riesgo aceptable, por lo que todos los activos con valor de riesgo inferior a {3} en el cálculo del riesgo no van a ser tratados por el momento. Con esto la dirección pretende dar prioridad a los activos que requieren de mayor y más rápida atención.

Una vez establecidos los controles para los riesgos por encima del nivel medio de criticidad reduciremos el riesgo pero este seguirá existiendo. El riesgo remanente después de aplicar los controles de seguridad se denomina riesgo residual, la herramienta PILAR nos calcula unos objetivos reales sobre el riesgo de nuestros activos aplicando los controles del Esquema Nacional de Seguridad, se trataría de una primera aproximación y aunque lo deseable es conseguir reducir el riesgo residual por debajo del riesgo aceptable, en algunos puntos aún aplicando los controles no va a ser posible, por lo que quedaría pendiente para la primera revisión del Plan de Adaptación al Esquema Nacional de Seguridad.

Riesgo Residual recomendado por PILAR por activo:

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[L.building_CC] Casa Consistorial	{3,1}	-	-	-	-
[L.building_CP] Centro Polivalente	{0,59}	-	-	-	-
[L.local_CPD] CPD Casa Consistorial	{3,1}	-	-	-	-
[L.building_SP] Satélite Policía	{0,59}	-	-	-	-
[L.ST] Servicios Técnicos	{0,82}	-	-	-	-
[L.building_ST] Servicios Técnicos	{0,82}	-	-	-	-
[L.channel_fibraST] Fibra Servicios Técnicos Casa Consistorial	{0,82}	-	-	-	-

activo	[D]	[I]	[C]	[A]	[T]
[L.BIBLIO] Biblioteca	{0,35}	-	-	-	-
[L.building_Biblioteca] Biblioteca	{0,35}	-	-	-	-
[L.channel_fibraB] Fibra Biblioteca Casa Consistorial	{0,35}	-	-	-	-

Tabla 29: AR - Riesgo Residual Activos Instalaciones

[SW] Aplicación

activo	[D]	[I]	[C]	[A]	[T]
[SW.Aplicaciones] Servidores de Aplicaciones	{1,2}	{2,5}	{2,5}	-	-
[SW.APP.Padron] WPadron	{1,2}	{2,5}	{2,5}	-	-
[SW.APP.Eurocop] Eurocop Servidor	{0,81}	{1,9}	{2,5}	-	-
[SW.APP.Nominas] A3Nom	{0,81}	{1,9}	{2,5}	-	-
[SW.APP.GLPI] Gestion Informática GLPI	{0,45}	{0,82}	{0,71}	-	-
[SW.APP.Impresion] Servidor Impresión MyQ	{0,45}	{0,47}	{0,48}	-	-
[SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo	{0,57}	{0,82}	{2,5}	-	-
[SW.www.Intranet] Servicio Intranet Local	{0,45}	{0,70}	{2,5}	-	-
[SW.office] Software Ofimática	{0,34}	{0,35}	{0,36}	-	-
[SW.office.Libre7] LibreOffice7	{0,34}	{0,35}	{0,36}	-	-
[SW.office.Office13ADV] Office 2013 advanced	{0,34}	{0,35}	{0,36}	-	-
[SW.office.Office13STA] Office 2013 standard	{0,34}	{0,35}	{0,36}	-	-
[SW.Clientes] Software Cliente	{0,92}	{0,93}	{0,94}	-	-
[SW.Other.Padron] Padrón Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.Eurocop] Eurocop Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.Lexnet] Lexnet Cliente	{0,22}	{0,23}	{0,71}	-	-
[SW.Other.Siltra] Siltra Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.ZKSoft] ZkSoftware Cliente Control Accesos	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.GIS] Software de Gestión Territorial Cliente	{0,92}	{0,93}	{0,94}	-	-
[SW.Other.Reca] ATM Recaudación Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.VNC] VNC Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.Conta] ATM Contabilidad Cliente	{0,22}	{0,23}	{0,48}	-	-
[SW.Other.AutoCAD19] Software Autocad 2019	{0,34}	{0,35}	{0,36}	-	-
[SW.Other.Presto] Software Presto 2019	{0,34}	{0,35}	{0,36}	-	-
[SW.Other.SondaProveedor] Sonda Servicio Proveedor Mantenimiento	{0,34}	{0,58}	{0,59}	-	-
[SW.Cloud] Software en Cloud	{1,2}	{1,9}	{2,5}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[SW.email_server.Postfix] Servidor Correo	{1,2}	{1,9}	{2,5}	-	-
[SW.www.Plesk_1] Servidor Plesk Correo	{1,2}	{1,9}	{2,5}	-	-
[SW.www.Plesk_2] Servidor Plesk Web	{1,2}	{1,9}	{0,71}	-	-
[SW.www.WebAyto] Servicio Wordpress	{1,2}	{1,9}	{0,71}	-	-
[SW.Pruebas] Servidores Pruebas	{0,10}	{0,11}	{0,71}	-	-
[SW.Other.Pruebas_2] Servidor Pruebas	{0,10}	{0,11}	{0,71}	-	-
[SW.Other.Pruebas_3] Servidor Pruebas	{0,10}	{0,11}	{0,71}	-	-
[SW.Other.Pruebas_1] Servidor Pruebas	{0,10}	{0,11}	{0,71}	-	-
[SW.Virtualización] Virtualización de Infraestructura y Escritorios	{2,4}	{2,5}	{2,5}	-	-
[SW.APP.VDIConnection_1] Servidor VDI Connection	{0,92}	{0,47}	{0,48}	-	-
[SW.APP.VDIConnection_3] Servidor VDI Connection	{0,92}	{0,47}	{0,48}	-	-
[SW.APP.VDIConnection_2] Servidor VDI Connection	{0,92}	{0,47}	{0,48}	-	-
[SW.APP.VDIComposer] Servidor VDI Composer	{0,34}	{0,47}	{0,48}	-	-
[SW.APP.VDISecurity] Servidor VDI Security	{0,92}	{0,93}	{0,94}	-	-
[SW.file.PerfilesVDI] Servidor ficheros de Perfiles VDI	{0,92}	{1,9}	{2,5}	-	-
[SW.hypervisor.Horizon7] Horizon VDI	{0,92}	{0,93}	{2,5}	-	-
[SW.hypervisor.vCenterInfra] vCenter Infraestructura	{2,4}	{2,5}	{2,5}	-	-
[SW.hypervisor.vCenterVDI] vCenter VDI	{0,92}	{0,93}	{2,5}	-	-
[SW.infra] Software de Infraestructura	{1,8}	{1,9}	{2,5}	-	-
[SW.directory.DC_1] Controlador Dominio DNS	{0,92}	{1,3}	{0,94}	-	-
[SW.directory.DC_2] Controlador Dominio DNS	{0,92}	{1,3}	{0,94}	-	-
[SW.directory.DHCP_1] Servidor DHCP	{0,92}	{0,47}	{0,48}	-	-
[SW.directory.DHCP_2] Servidor DHCP	{0,92}	{0,47}	{0,48}	-	-
[SW.APP.KMS] Servidor Licencias Microsoft	{0,34}	{0,47}	{0,71}	-	-
[SW.APP.WSUS] Servidor Actualizaciones Microsoft	{0,34}	{0,35}	{0,36}	-	-
[SW.file.Ficheros] Servidor de Ficheros	{1,8}	{1,9}	{2,5}	-	-
[SW.Other.Santricity] Gestor de Storage	{0,10}	{0,11}	{0,12}	-	-
[SW.backup] Software de Backup	{1,2}	{1,9}	{2,5}	-	-
[SW.backup.Backup_1] Servidor VDP Backup	{1,2}	{1,9}	{2,5}	-	-
[SW.backup.Backup_2] Servidor VDP Backup	{1,2}	{1,9}	{2,5}	-	-
[SW.dbms.SQL12] Servidor SQL Server 2012	{2,4}	{2,5}	{2,5}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[SW.seguridad] Software de seguridad	{1,2}	{1,3}	{1,3}	-	-
[SW.AV.SophosServer] Sophos Advanced Server	{1,2}	{1,3}	{1,3}	-	-
[SW.AV.SophosFisicos] Sophos Standard Equipos Físicos	{0,81}	{0,82}	{0,83}	-	-
[SW.AV.SophosVDI] Sophos Advanced VDI	{0,81}	{0,82}	{0,83}	-	-
[SW.APP.ServerEndpoint_2] Servidor Sophos Endpoint	{1,2}	{1,3}	{1,3}	-	-
[SW.APP.ServerEndpoint_1] Servidor Sophos Endpoint	{1,2}	{1,3}	{1,3}	-	-
[SW.OS.WIN12] Server 2012 R2	{2,4}	{2,5}	{2,5}	-	-
[SW.OS.WIN16] Server 2016 VDI	{0,34}	{0,35}	{0,36}	-	-
[SW.OS.WIN10] Windows 10	{0,34}	{0,35}	{0,36}	-	-
[SW.OS.CENT7] Server Linux Centos 7	{1,2}	{1,9}	{2,5}	-	-

Tabla 30: AR - Riesgo Residual Activos Aplicación

[S] Servicios

activo	[D]	[I]	[C]	[A]	[T]
[S.cloud.SophosCentral] Central Endpoint Cloud de Sophos	{1,2}	{1,1}	{1,1}	{2,2}	{2,8}
[S.other.Mantenimiento] Mantenimiento para el CPD	{0,92}	{2,3}	{2,3}	{2,2}	{2,8}
[S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes	{2,4}	{2,3}	{2,3}	{2,2}	{2,8}
[S.iaas.MailWeb] Proveedor de Infraestructura como Servicio	{1,8}	{1,7}	{2,3}	{2,2}	{2,8}
[S.ca.Certs] Proveedor de certificados FNMT	{0,81}	{0,78}	{0,78}	{2,2}	{0,88}
[S.other.Soporte] Proveedores de soporte de aplicaciones	{0,57}	{0,90}	{0,90}	{0,89}	{2,8}
[S.isp.Internet] Proveedor de acceso a Internet	{2,9}	{1,7}	{2,3}	{2,2}	{2,8}

Tabla 31: AR - Riesgo Residual Activos Servicios

[AUX] Equipamiento Auxiliar

activo	[D]	[I]	[C]	[A]	[T]
[AUX.CPD] elementos del CPD	{1,6}	{0,43}	{1,1}	-	-
[AUX.ups.CPD_2] UPS del CPD	{0,69}	-	-	-	-
[AUX.ac.CPD_2] Split de Aire Acondicionado del CPD	{1,2}	-	-	-	-
[AUX.furniture.RackCPD_2] Rack CPD	{0,99}	{0,01}	{0,09}	-	-
[AUX.furniture.RackCPD_1] Rack CPD	{0,99}	{0,01}	{0,09}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[AUX.furniture.Armario] Armario Ignífugo Caja Fuerte	{0,17}	{0,01}	{1,1}	-	-
[AUX.ac.CPD_1] Split de Aire Acondicionado del CPD	{1,2}	-	-	-	-
[AUX.ups.CPD_1] UPS del CPD	{0,69}	-	-	-	-
[AUX.other.Extintor] Extintor de CO2	{0,17}	{0,01}	{0,09}	-	-
[AUX.other.AccesoCPD] Sistema de control de acceso con alarma al CPD	{1,6}	{0,43}	{1,1}	-	-
[AUX.ups.SatPolicia] Mini UPS del Satélite de Policía	{0,01}	-	-	-	-
[AUX.ups.CentroPol] Mini UPS del Centro Polivalente	{0,01}	-	-	-	-

Tabla 32: AR - Riesgo Residual Activos Equipamiento Auxiliar

[HW] Hardware

activo	[D]	[I]	[C]	[A]	[T]
[HW.CPD] Equipos del CPD	{3,1}	{2,8}	{2,8}	-	-
[HW.CPD.INFRA] HW Virtualización Equipos Infraestructura	{3,1}	{2,8}	{2,8}	-	-
[HW.host.INFRA_2] ESX Infraestructura	{3,1}	{0,98}	{2,1}	-	-
[HW.host.INFRA_1] ESX Infraestructura	{3,1}	{0,98}	{2,1}	-	-
[HW.data.CabinaProd] Cabina de Producción	{3,1}	{2,8}	{2,8}	-	-
[HW.vhost.Switch] Switch Virtual Servidores Infraestructura	{3,1}	{0,28}	{0,52}	-	-
[HW.data.DataStores_3] DataStores Virtuales Equipos Infraestructura	{3,1}	{2,8}	{2,8}	-	-
[HW.data.DataStores_2] DataStores Virtuales Backup	{2,5}	{2,2}	{2,8}	-	-
[HW.data.CabinaBack] Cabina de Backup	{2,5}	{2,2}	{2,8}	-	-
[HW.vhost.Servidores] Máquinas Virtuales Servidores Infraestructura	{3,1}	{0,98}	{2,1}	-	-
[HW.CPD.VDI] Hardware Virtualización de Escritorios	{1,3}	{1,0}	{2,8}	-	-
[HW.host.VDI_2] ESX VDI	{0,94}	{0,39}	{0,64}	-	-
[HW.host.VDI_3] ESX VDI	{0,94}	{0,39}	{0,64}	-	-
[HW.host.VDI_1] ESX VDI	{0,94}	{0,39}	{0,64}	-	-
[HW.data.DataStores_1] DataStores Virtuales Escritorios Usuarios vSAN	{1,3}	{1,0}	{2,8}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[HW.vhost.Switch_1] Switch Virtual Escritorios Usuarios	{1,3}	{0,28}	{0,52}	-	-
[HW.vhost.VDI] Máquinas Virtuales Escritorios Usuarios	{0,48}	{0,04}	{0,87}	-	-
[HW.CPD.COM] Comunicaciones CPD	{3,1}	{0,98}	{2,2}	-	-
[HW.other.Firewall_2] Firewall en HA	{2,5}	{0,86}	{2,2}	-	-
[HW.other.Firewall_1] Firewall en HA	{2,5}	{0,86}	{2,2}	-	-
[HW.Other.SwitchStack] Core Switch Stack 10G	{3,1}	{0,98}	{2,1}	-	-
[HW.switch.SwitchCPD_2] Switch de Usuario CPD	{0,94}	{0,28}	{0,52}	-	-
[HW.switch.SwitchCPD_1] Switch de Usuario CPD	{0,94}	{0,28}	{0,52}	-	-
[HW.router.CPD_2] Router ADSL Servicio Correo Postal	{0,48}	{0,28}	{0,87}	-	-
[HW.router.CPD_3] Router ADSL Red SARA	{0,71}	{0,63}	{2,1}	-	-
[HW.router.CPD_1] Router Fibra Principal CPD	{2,5}	{0,63}	{0,87}	-	-
[HW.CentroPol] Equipos Centro Polivalente	{0,59}	{0,86}	{1,6}	-	-
[HW.other.MiniFW_2] Firewall Centro Polivalente	{0,59}	{0,86}	{1,6}	-	-
[HW.router.CentroPol] Router Fibra Centro Polivalente	{0,59}	{0,86}	{1,6}	-	-
[HW.switch.SwitchST] Switch de Usuario Servicios Técnicos	{0,94}	{0,28}	{0,52}	-	-
[HW.SatPolicia] Equipos Satélite Policía	{0,59}	{0,86}	{1,6}	-	-
[HW.router.SatPolicia] Router Fibra Satélite Policía	{0,59}	{0,86}	{1,6}	-	-
[HW.other.MiniFW_1] Firewall Satélite Policía	{0,59}	{0,86}	{1,6}	-	-
[HW.switch.SwitchCCP2] Switch de Usuario Casa Consistorial P2	{0,94}	{0,28}	{0,52}	-	-
[HW.switch.SwitchBiblio] Switch de Usuario Biblioteca	{0,59}	{0,28}	{0,52}	-	-
[HW.pc.ZeroClient] Equipos de Usuarios Virtualizados	{0,48}	{0,04}	{0,87}	-	-
[HW.pc.Equipo] Equipos de Usuarios	{0,48}	{0,04}	{0,64}	-	-
[HW.mobile.PortatilTeletrabajo] Equipo Portátil para Teletrabajo	{0,48}	{0,05}	{0,87}	-	-
[HW.print.Impresoras] Impresoras	{0,83}	{0,04}	{0,65}	-	-
[HW.vhost.Cloud] Máquinas Virtuales Servidores Infraestructura Cloud	{1,9}	{0,86}	{2,1}	-	-

Tabla 33: AR - Riesgo Residual Activos Hardware

[COM] Red

activo	[D]	[I]	[C]	[A]	[T]
[COM.CentroPol] Comunicaciones Centro Polivalente	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.other.CentroPol] Túnel Centro Polivalente CPD	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.wan.CentroPol] WAN del Centro Polivalente	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.SatPolicia] Comunicaciones Satélite Policía	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.other.SatPolicia] Túnel Satélite Policía CPD	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.wan.SatPolicia] WAN del Satélite Policía	{0,62}	{0,99}	{1,8}	{2,3}	-
[COM.CPD] Comunicaciones CPD	{3,2}	{1,6}	{2,4}	{2,9}	-
[COM.vpn.RedSara] VPN con la Red Sara	{0,74}	{0,76}	{2,4}	{2,9}	-
[COM.other.Teletrabajo] Conexión contra servidor de seguridad PCoIP	{1,5}	{0,76}	{0,92}	{2,9}	-
[COM.vpn.RedMonitor] VPN con la Red de Monitorización para mantenimiento	{0,50}	{0,40}	{0,56}	{0,67}	-
[COM.adsl.CPD_2] ADSL Correos Postal IP fija	{0,50}	{0,40}	{0,92}	{0,44}	-
[COM.wan.CPD] WAN del CPD	{2,7}	{0,76}	{0,92}	{2,9}	-
[COM.vlan.ILO] VLAN para las ilos de los hosts	{0,50}	{0,40}	{0,33}	{1,2}	-
[COM.vlan.VSAN] VLAN para el servicio de vSAN	{0,97}	{0,40}	{0,33}	{0,67}	-
[COM.adsl.CPD_1] ADSL Red Sara IP fija	{0,74}	{0,76}	{2,4}	{2,9}	-
[COM.vlan.EquiposInfra] VLAN para los Equipos de Infraestructura	{3,2}	{1,6}	{2,4}	{2,9}	-
[COM.vlan.EquiposUsuario] VLAN para los usuarios de Usuario Interno	{2,7}	{0,99}	{1,8}	{1,2}	-
[COM.vlan.EquiposMancomunidad] VLAN para los usuarios de la Mancomunidad	{0,62}	{0,29}	{2,4}	{1,2}	-

Tabla 34: AR - Riesgo Residual Activos Red

[P] Personal

activo	[D]	[I]	[C]	[A]	[T]
[P.ui.Oper] Usuarios Operadores del Sistema	{0,87}	{0,92}	{0,96}	-	-
[P.prov] Usuarios Proveedores	{1,2}	{2,4}	{2,4}	-	-
[P.prov.Oper] Usuarios Proveedores Operadores del Sistema	{0,68}	{0,92}	{0,92}	-	-
[P.prov.Admins] Usuarios Proveedores Administradores del Sistema	{1,2}	{2,4}	{2,4}	-	-

activo	[D]	[I]	[C]	[A]	[T]
[P.adm.Admins] Usuarios Administradores del Sistema	{2,3}	{2,8}	{3,3}	-	-
[P.ui.UsuInternos] Usuarios Internos	{0,52}	{0,69}	{0,73}	-	-
[P.ue.Oposicion] Usuarios miembros de la Oposición Política	{0,01}	{0,45}	{0,33}	-	-
[P.ue.Mancomunidad] Usuarios de la Mancomunidad	{0,01}	{0,69}	{0,57}	-	-

Tabla 35: AR - Riesgo Residual Activos Personal

[D] Datos

activo	[D]	[I]	[C]	[A]	[T]
[D.Virtualizacion] Datos relacionados con la Virtualización	{1,4}	{2,3}	{4,1}	{3,7}	-
[D.conf.Virtualización] BD de los vCenters	{0,84}	{0,85}	{0,85}	{2,0}	-
[D.files.PerfilesVDI] Datos de los Escritorios de VDI	{1,4}	{2,3}	{4,1}	{3,7}	-
[D.conf.PlantillasVDI] Plantillas VDI	{0,37}	{0,85}	{0,49}	{0,60}	-
[D.logs.VDI] Logs de los vCenters y Horizon	{0,14}	{1,9}	{0,92}	{0,83}	-
[D.files.ServFicheros] Datos en Unidades de Red Compartidas	{0,72}	{2,3}	{4,1}	{3,7}	-
[D.backup.Respaldos] Datos de las copias de Seguridad	{0,61}	{2,3}	{4,1}	{3,7}	-
[D.BDSQLServer] BD contenidas en el servidor de SQL	{0,61}	{2,3}	{4,1}	{3,7}	-
[D.files.BD_Contabilidad] BD Aplicación Contabilidad	{0,61}	{2,3}	{4,1}	{3,7}	-
[D.files.BD_Recaudacion] BD Aplicación Recaudación	{0,61}	{2,3}	{4,1}	{3,7}	-
[D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos	{0,02}	{0,79}	{2,4}	{2,0}	-
[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo	{0,14}	{0,91}	{4,1}	{3,7}	-
[D.files.BD_GIS] BD Aplicación GIS	{0,49}	{1,2}	{2,4}	{2,0}	-
[D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware	{0,01}	{0,79}	{2,4}	{0,95}	-
[D.files.BD_Padron] BD Aplicación WPadron	{0,61}	{2,9}	{4,1}	{3,7}	-
[D.files.BD_Nominas] BD Aplicación A3Nom	{0,37}	{2,3}	{4,1}	{3,7}	-
[D.conf.GPO] Datos de configuración de las GPOs	{0,61}	{0,85}	{0,49}	{2,0}	-
[D.files.BD_Eurocop] BD Aplicación Eurocop	{0,37}	{2,3}	{4,1}	{3,7}	-
[D.logs.Windows] Logs de Windows	{0,01}	{1,9}	{0,68}	{0,60}	-

Tabla 36: AR - Riesgo Residual Activos Datos

Toda la información de riesgo aceptable y riesgo residual queda documentada en el “Acta de Aceptación de Riesgos por la Dirección” que se adjuntará como anexo al Plan de Adaptación al ENS (no incluida en este TFM).

4.2. Categorización del Sistema de acuerdo con el ENS

Para desarrollarla se emplea como base la Guía de Seguridad de las TIC CCN-STIC 883 para Ayuntamientos menores de 20.000 habitantes [18].

Ver producto obtenido del TFM (Categorización del sistema.pdf)

El documento de categorización del sistema es obligatorio dentro del Plan de Adaptación al ENS.

Vamos a resaltar la equivalencia entre los activos de información de la Categorización del Sistema con los activos de Datos [D] del Análisis de Riesgos. Todos los activos de la categorización del sistema incluyen información en los siguientes activos: “[D.files.ServFicheros] Datos en Unidades de Red Compartidas”, “[D.backup.Respaldos] Datos de las copias de Seguridad”, “[D.files.PerfilesVDI] Datos de los Escritorios de VDI”, “[D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo” y en el gestor de expedientes municipal “[S.saas.GestorExpedientes] Proveedor del Gestor de Expediente” así como en la infraestructura física y lógica que los soporta. En la siguiente tabla indicamos las excepciones:

Categorización del Sistema	Activos Análisis de Riesgos
I01 - GESTIÓN URBANISMO MUNICIPAL	[D.files.BD_GIS] BD Aplicación GIS
I02 - LICENCIAS, AUTORIZACIONES Y CONCESIONES	[D.files.BD_GIS] BD Aplicación GIS
I03 - ATENCIÓN A LA CIUDADANÍA	-
I04 - ATENCIONES Y PRESTACIONES SOCIALES	-
I05 - AYUDAS Y SUBVENCIONES	-
I06 - POLICÍA LOCAL	[D.files.BD_Eurocop] BD Aplicación Eurocop
I07 - PROTECCIÓN CIVIL	-
I08 - PROCEDIMIENTOS SANCIONADORES	-
I09 - SERVICIOS TELEMÁTICOS Y COMUNICACIONES	-
I10 - GESTIÓN DE SERVICIOS FUNERARIOS	-
I11 - GESTIÓN DE INGRESOS	[D.files.BD_Recaudacion] BD Aplicación

Categorización del Sistema	Activos Análisis de Riesgos
PÚBLICOS	Recaudación
I12 - GESTIÓN DE SERVICIOS DEPORTIVOS	-
I13 - GESTIÓN DE SERVICIOS CULTURALES	-
I14 - GESTIÓN DE SERVICIOS EDUCATIVOS	-
I15 - GESTIÓN DEL ARCHIVO MUNICIPAL	-
I16 - CONTRATACIÓN PÚBLICA	-
I17 - GESTIÓN DEL PERSONAL	[D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware [D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos [D.files.BD_Nominas] BD Aplicación A3Nom
I18 - GESTIÓN PRESUPUESTARIA ECONÓMICA Y CONTABLE	[D.files.BD_Contabilidad] BD Aplicación Contabilidad
I19 - GESTIÓN DE LOS ÓRGANOS MUNICIPALES DE GOBIERNO	-
I20 - PADRÓN MUNICIPAL DE HABITANTES	[D.files.BD_Padron] BD Aplicación WPadron
I21 - REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS	-
I22 - DEFENSA JURÍDICA Y RESPONSABILIDAD PATRIMONIAL	-
I23 - SEGURIDAD DE INSTALACIONES MUNICIPALES	-
I24 - GESTIÓN DE SERVICIOS JUVENILES MUNICIPALES	-
I25 - GESTIÓN DE LA PARTICIPACIÓN CIUDADANA	-
I26 - VOLUNTARIADO	-
I27 - GESTIÓN DE LAS OBRAS MANTENIMIENTO E INFRAESTRUCTURAS	[D.files.BD_GIS] BD Aplicación GIS
I28 - GESTIÓN DE LA PROMOCIÓN LOCAL Y EL TURISMO	-
I29 - GESTIÓN DE ACTIVIDADES EN TRANSPARENCIA	-
I30 - SISTEMAS DE INFORMACIÓN Y	[D.Virtualizacion] Datos relacionados con

Categorización del Sistema	Activos Análisis de Riesgos
COMUNICACIONES	la Virtualización *(contenedor de activos)* [D.conf.GPO] Datos de configuración de las GPOs [D.logs.Windows] Logs de Windows

Tabla 37: Relación específica entre Activos de la Categorización del Sistema y Activos identificados en el Análisis de Riesgos

4.3. Calidad del Dato

A continuación ejecutaremos la evaluación de los activos que contienen datos evaluables aplicando los criterios establecidos en el apartado 3.10.2.

4.3.1. Identificación de activos evaluables

Esta evaluación se centra exclusivamente en los activos pertenecientes a la categoría Datos [D] y Servicios [S], de entre todos estos activos vamos a seleccionar aquellos que contengan datos personales tal y como identificamos en el apartado 4.2.3. por lo tanto los activos evaluables serán los siguientes:

- [D.files.PerfilesVDI] Datos de los Escritorios de VDI
- [D.files.ServFicheros] Datos en Unidades de Red Compartidas
- [D.backup.Respaldos] Datos de las copias de Seguridad
- [D.files.BD_Contabilidad] BD Aplicación Contabilidad
- [D.files.BD_Recaudacion] BD Aplicación Recaudación
- [D.files.BD_Intranet] BD de la Intranet Vacaciones y Permisos
- [D.files.BD_GestorExpAntiguo] BD del Gestor de Expedientes Antiguo
- [D.files.BD_GIS] BD Aplicación GIS
- [D.acl.BD_ZKSoft] BD Control de Accesos Zksoftware
- [D.files.BD_Padron] BD Aplicación Wpadron
- [D.files.BD_Nominas] BD Aplicación A3Nom
- [D.files.BD_Eurocop] BD Aplicación Eurocop
- [S.saas.GestorExpedientes] Proveedor del Gestor de Expedientes
- [S.iaas.MailWeb] Proveedor de Infraestructura como Servicio

Aunque se analicen únicamente datos y servicios los resultados abarcan el viaje de estos hacia los distintos software cliente asociados, no se limitan, por ejemplo en el caso de una BD, únicamente al fichero o ficheros de la propia BD.

4.3.2. Valoración de los activos

[D.files.PerfilesVDI]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	Emplea recursos propios del Ayuntamiento. Está cercano a “Excede los Requerimientos”
Conformidad	Mínimamente Aceptable	-
Trazabilidad	Excede los requerimientos	Trazabilidad de 2 meses
Confidencialidad	Rango Objetivo	-
Disponibilidad	Rango Objetivo	-

Tabla 38: CD - Evaluación Datos de los Escritorios de VDI

[D.files.ServFicheros]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	Emplea recursos propios del Ayuntamiento. Está cercano a “Excede los Requerimientos”
Conformidad	Mínimamente Aceptable	-
Trazabilidad	Excede los requerimientos	Trazabilidad de 2 meses
Confidencialidad	Rango Objetivo	-
Disponibilidad	Rango Objetivo	-

Tabla 39: CD - Evaluación Datos en Unidades de Red Compartidas

[D.backup.Respaldos]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	Emplea recursos propios del Ayuntamiento. Está cercano a “Excede los Requerimientos”
Conformidad	Mínimamente Aceptable	-
Trazabilidad	Excede los requerimientos	Trazabilidad de 2 meses
Confidencialidad	Rango Objetivo	-
Disponibilidad	Rango Objetivo	-

Tabla 40: CD - Evaluación Datos de las copias de Seguridad

[D.files.BD_Contabilidad]	Valor	Observaciones
Recuperabilidad	Inaceptable	En caso de error, el tiempo de respuesta del soporte puede rondar las 24 horas. El Dep. de informática en caso de urgencia podría reponer un backup pero a costa de posibles inconsistencias y pérdida de trabajo realizado
Conformidad	Inaceptable	El proveedor no tiene planes a corto plazo de adaptar su software ni la forma de trabajar con la BD al ENS ni al ENI
Trazabilidad	Inaceptable	No hay trazabilidad de operaciones en la BD
Confidencialidad	Inaceptable	-
Disponibilidad	Mínimamente Aceptable	-

Tabla 41: CD - Evaluación BD Aplicación Contabilidad

[D.files.BD_Recaudacion]	Valor	Observaciones
Recuperabilidad	Inaceptable	En caso de error, el tiempo de respuesta del soporte ronda las 24 horas. El Dep. de informática en caso de urgencia podría reponer un backup pero a costa de posibles inconsistencias y pérdida de trabajo realizado en el día, problemático si se han ejecutado procesos complejos
Conformidad	Inaceptable	El proveedor no tiene planes a corto plazo de adaptar su software ni la forma de trabajar con la BD al ENS ni al ENI
Trazabilidad	Inaceptable	No hay trazabilidad de operaciones en la BD
Confidencialidad	Inaceptable	-
Disponibilidad	Mínimamente Aceptable	-

Tabla 42: CD - Evaluación BD Aplicación Recaudación

[D.files.BD_Intranet]	Valor	Observaciones
Recuperabilidad	Inaceptable	No cuenta con soporte. El Dep. de informática en caso de urgencia podría reponer un backup pero a costa de posibles inconsistencias y pérdida de datos del día
Conformidad	Inaceptable	Software descatalogado desde 2016
Trazabilidad	Mínimamente Aceptable	-
Confidencialidad	Inaceptable	-
Disponibilidad	Mínimamente Aceptable	

Tabla 43: CD - Evaluación BD de la Intranet Vacaciones y Permisos

[D.files.BD_GestorExpAntiguo]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	No cuenta con soporte. El Dep. de informática en caso de urgencia podría reponer un backup. Los datos no se actualizan en esta BD
Conformidad	Inaceptable	Software descatalogado desde 2018
Trazabilidad	Rango Objetivo	-
Confidencialidad	Mínimamente Aceptable	-
Disponibilidad	Rango Objetivo	-

Tabla 44: CD - Evaluación BD del Gestor de Expedientes Antiguo

[D.files.BD_GIS]	Valor	Observaciones
Recuperabilidad	Mínimamente aceptable	Tiempo de respuesta de soporte de menos de 8 horas
Conformidad	Mínimamente aceptable	-
Trazabilidad	Rango Objetivo	-
Confidencialidad	Mínimamente Aceptable	-
Disponibilidad	Rango Objetivo	-

Tabla 45: CD - Evaluación BD Aplicación GIS

[D.acl.BD_ZKSoft]	Valor	Observaciones
Recuperabilidad	Inaceptable	No cuenta con soporte. El Dep. de informática en caso de urgencia podría reponer un backup pero a costa de posibles inconsistencias y pérdida de datos del día
Conformidad	Inaceptable	Software descatalogado desde 2019
Trazabilidad	Mínimamente Aceptable	-
Confidencialidad	Inaceptable	-
Disponibilidad	Rango Objetivo	-

Tabla 46: CD - Evaluación BD Control de Accesos Zksoftware

[D.files.BD_Padron]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	Recuperable en menos de 2 horas
Conformidad	Rango Objetivo	-
Trazabilidad	Rango Objetivo	-
Confidencialidad	Excede los Requerimientos	-
Disponibilidad	Rango Objetivo	-

Tabla 47: CD - Evaluación BD Aplicación Wpadron

[D.files.BD_Nominas]	Valor	Observaciones
Recuperabilidad	Mínimamente Aceptable	Recuperable en menos de 8 horas
Conformidad	Mínimamente Aceptable	-
Trazabilidad	Mínimamente Aceptable	-
Confidencialidad	Rango Objetivo	-
Disponibilidad	Rango Objetivo	-

Tabla 48: CD - Evaluación BD Aplicación A3Nom

[D.files.BD_Eurocop]	Valor	Observaciones
Recuperabilidad	Rango Objetivo	Recuperable en menos de 2 horas
Conformidad	Rango Objetivo	-
Trazabilidad	Rango Objetivo	-
Confidencialidad	Rango Objetivo	-
Disponibilidad	Rango Objetivo	-

Tabla 49: CD - Evaluación BD Aplicación Eurocop

[S.saas.GestorExpedientes]	Valor	Observaciones
Recuperabilidad	Excede los requerimientos	-
Conformidad	Excede los requerimientos	-
Trazabilidad	Excede los requerimientos	-
Confidencialidad	Excede los requerimientos	-
Disponibilidad	Excede los requerimientos	-

Tabla 50: CD - Evaluación Proveedor del Gestor de Expedientes

[S.iaas.MailWeb]	Valor	Observaciones
Recuperabilidad	Excede los requerimientos	-
Conformidad	Excede los requerimientos	-
Trazabilidad	Rango Objetivo	-
Confidencialidad	Excede los requerimientos	-
Disponibilidad	Rango Objetivo	-

Tabla 51: CD - Evaluación Proveedor de Infraestructura como Servicio

4.3.3. Nivel de Calidad del Dato Aceptable (Resultado Evaluación)

En el Procedimiento de Revisión por Dirección se lleva como punto de la reunión la Evaluación de la Calidad del Dato (se facilita el Informe de Calidad del Dato con antelación) y la aprobación del Nivel de Calidad del Dato Aceptable. Una vez estudiada la evaluación por la gerencia se establece el nivel “Mínimamente Aceptable” dentro de los niveles de evaluación del punto 3.10.2. “Resultados de la Evaluación” como el nivel mínimo de calidad del Dato Aceptable desde el cual merece la pena aplicar las propuestas de mejora, los activos con nivel de calidad del dato inferior no van a ser tratados y se propondrá su cambio por otros nuevos que sí cumplan con el nivel mínimo de calidad del dato. Con esto la dirección pretende centrar esfuerzos en los activos que requieran menor esfuerzo a la hora de mejorar la calidad del dato y no perder tiempo en aquellos que es mejor cambiar antes que mejorar. Recordemos que para que un activo se considere dentro del nivel “Mínimamente Aceptable” tiene que tener este mismo nivel para todas las características de calidad del dato consideradas en la evaluación: Recuperabilidad, Conformidad, Trazabilidad, Confidencialidad y Disponibilidad. Finalmente se establece que el activo [SW.APP.ExpAntiguo] Gestor de Expedientes Antiguo, al tratarse de un servidor en desuso, sin posibilidad de migración, pero que se tiene que mantener para consultas, quedará excluido de esta valoración y se permitirá su inclusión dentro de los proyectos de mejora de la seguridad en el grado en que este servidor lo permita, además se tomarán medidas de seguridad adicionales como por ejemplo que este se encuentre disponible (encendido) sólo en ciertas franjas horarias y ciertos días.

Por lo tanto los activos con valoración “Inaceptable” son los siguientes: [D.files.BD_Contabilidad], [D.files.BD_Recaudacion], [D.files.BD_Intranet], y [D.acl.BD_ZKSoft].

5. Propuesta de Proyectos

Llegados a este punto hemos estudiado el estado inicial del Ayuntamiento, hemos definido toda la documentación necesaria y hemos llevado a cabo un análisis de riesgos, con toda esta información es el momento de realizar propuestas de mejora de la seguridad con el fin de aprovechar todo este trabajo.

5.1. Proyectos Prioritarios

Durante la elaboración de este TFM hemos realizado proyectos prioritarios como son el desarrollo de la Política de Seguridad, la Categorización del Sistema, realizar el Análisis de Riesgos, realizar la Declaración de Aplicabilidad o el Plan de Mejora de la Seguridad. Todos estos proyectos se encuentran documentados en el **producto obtenido "Plan de mejora de la seguridad.pdf"** donde incluso encontraremos más proyectos de los que existen en este apartado del TFM, esto es debido a que exponemos los proyectos a implantar y no los ya conseguidos.

* Todos los activos marcados con asterisco quedarán fuera del proyecto por sus resultados en la evaluación de la Calidad del Dato, ya que se van a sustituir por nuevos proyectos.

Código: P-01-2020	**Nombre**: Plan de formación en seguridad
Objetivos: Desarrollar y aprobar la normativa de seguridad de los recursos TIC (correo, internet, etc.) puestos a disposición del personal que regule también, entre otros, el uso de dispositivos portátiles, soportes extraíbles, la necesidad de que los usuarios bloqueen su puesto de trabajo ante las ausencias, la necesidad de limpiar los documentos de metadatos no necesarios, etc. Aprobar formalmente y difundir a todo personal: publicación en la intranet municipal. Elaborar de plan anual de difusión/sensibilización y de formación.	
Situación específica del Ayuntamiento: Actualmente la plantilla del Ayuntamiento de la UOC es el eslabón más débil de la organización y a pesar de los esfuerzos del departamento de informática mediante circulares y otros mecanismos de difusión, no se está consiguiendo una concienciación efectiva de los usuarios. El responsable de seguridad será el encargado del desarrollo de la normativa de seguridad, trabajará junto con el responsable de RRHH para elaborar el plan anual de difusión/sensibilización en seguridad de la información. Mediante contrato menor se contratará una empresa de formación que creará elementos gráficos de impacto, estos serán usados en sus sesiones de formación que sucederán al menos una vez al año de forma física y además contará con una plataforma de teleformación donde los usuarios podrán acceder bajo asignación a los recursos de	

formación durante un tiempo limitado.	
Activos involucrados: • [P.ui.Oper] • [P.ui.UsuInternos] • [P.ue.Oposicion] • Recomendado: [P.ue.Mancomunidad]	**Responsables**: • RSEG • CSI
Controles ENS: • org.2 • mp.eq.1 • mp.eq.2 • mp.eq.3 • mp.si • mp.info.6 • mp.per.3 • mp.per.4	**Controles ISO/IEC 27001**: • 5.1 • 6.2 • 7.2.2 • 8.1.3 • 8.3.1 • 8.3.3 • 11.2.6 • 11.2.8 • 11.2.9 • 13.2.1 • 16.1.1 • 18.2.2

Tabla 52: Proyecto - Plan de formación en seguridad

Código: P-02-2020	**Nombre**: Procedimiento de gestión de la seguridad con terceros
Objetivos: Desarrollar e implantar un procedimiento de gestión de la seguridad con terceros: antes, durante y después de la contratación: Requisitos de solvencia técnica. Exigencia de declaración/certificación de conformidad con el ENS, contratos de encargado del tratamiento de datos personales y/o confidencialidad, acuerdos de nivel de servicio, etc. Inventariar terceros y regular su situación. En caso de servicios externalizados: completar con certificados de Conformidad ENS de los servicios subcontratados por el órgano competente. Para la gestión diaria completar con los Informes/herramientas seguimiento SLA proporcionadas por el órgano competente.	
Situación específica del Ayuntamiento: Si bien actualmente el Ayuntamiento de la UOC es estricto requiriendo la solvencia técnica a las empresas que trabajan para él, esta realmente no se encuentra consensuada y se limita a lo estipulado desde hace décadas por los departamentos jurídicos del Ayuntamiento, será necesario trabajar conjuntamente con el fin de tener actualizado esta información. Actualmente en los pliegos se exige conformidad con el ENS, acuerdos de nivel de servicio, etc. no obstante esto no se encuentra documentado y se hace más por intuición que por metodología. Si bien la mayoría de los terceros que trabajan con el Ayuntamiento se encuentran en situación regular, sí que existen algunos contratos que por acumulación de trabajo no se han podido regularizar aunque siguen prestándose al tratarse de servicios esenciales, será necesaria la contratación interina por acumulación de tareas de un técnico informático medio con nivel mínimo 23 (RSIS) que consiga eliminar este atasco para poder regularizar la situación. Se necesitará habilitar la herramienta GLPI de la que dispone el Ayuntamiento para el seguimiento de los SLAs proporcionados por las empresas que trabajan para el Ayuntamiento.	

Activos involucrados: • Todos los de la capa [S] Servicios • [P.prov.Oper] • [P.prov.Admins] • [SW.APP.Padron] y relacionados • [SW.APP.Eurocop] y relacionados • [SW.APP.Nominas] y relacionados • [SW.APP.Impresion] y relacionad. • * [SW.Other.Reca] y relacionados • * [SW.Other.Conta] y relacionados	**Responsable**: • CSI
Controles ENS: • op.ext.1 • op.ext.2	**Controles ISO/IEC 27001**: • 13.2.2 • 15.1 • 15.2

Tabla 53: Proyecto - Procedimiento de gestión de la seguridad con terceros

Código: P-03-2020	**Nombre**: Procedimiento de Protección frente a código dañino
Objetivos: Revisar las medidas de protección frente a código dañino, en todo el equipamiento incluido: el de las sedes, portátiles, etc. Se revisará el EDR (Endpoint Defense and Response) del Ayuntamiento. Desarrollar un procedimiento que describa la forma en la cual se gestiona y se mantiene la solución de protección frente a código dañino.	
Situación específica del Ayuntamiento: Si bien el Ayuntamiento de la UOC cuenta con un sistema Endpoint avanzado y continuamente actualizado es cierto que este no se encuentra documentado ni configurado al 100% de sus capacidades, por lo que será necesario realizar una revisión a fondo haciendo especial hincapié en las interconexiones entre los distintos elementos (firewalls, servidores, antivirus, etc.) de modo que se creen reacciones avanzadas ante la detección de materialización de amenazas, como por ejemplo el aislamiento de máquinas VDI ante la falta de heartbeat. Para este análisis el Ayuntamiento, una vez realizada la documentación y ajustadas las configuraciones, contratará un servicio de consultoría que perpetre las pruebas de pentesting necesarias mediante simulaciones de ataques (BAS) por los distintos medios de entrada, en la contratación se premiará el ofertar herramientas open source.	
Activos involucrados: • Todos los activos incluidos en el grupo [SW.seguridad] • [HW.other.Firewall_2] • [HW.other.Firewall_1] • [HW.other.MiniFW_1] • [HW.other.MiniFW_2] • [S.cloud.SophosCentral] • [S.other.Mantenimiento]	**Responsable**: • RSIS • RSEG (contratación)
Controles ENS: • op.exp.6	**Controles ISO/IEC 27001**: • 12.2.1

Tabla 54: Proyecto - Procedimiento de Protección frente a código dañino

Código: P-04-2020	**Nombre**: Procedimiento de Segmentación de redes
Descripción: Segmentar las redes de tal forma que cada equipo solamente tenga acceso a la información que necesita, se compartimenten los diferentes grupos de usuarios para evitar la propagación de malware y las redes de infraestructura e inalámbricas disponga de su propio segmento de red. Desarrollar los procedimientos asociados.	
Situación específica del Ayuntamiento: Si bien el Ayuntamiento tiene una red ciertamente segmentada, esta no se encuentra en su estado óptimo, pudiendo por ejemplo segmentar mejor la red de infraestructura añadiendo vlans exclusivas para: servidores de aplicaciones, servidores de infraestructura, infraestructura de red, infraestructura de storage, elementos de virtualización de servidores, elementos de virtualización de VDI, etc. Además es necesario documentar el estado de las vlans y su función.	
Activos involucrados: • Todos los activos de tipo vlan del grupo [COM. CPD] • [HW.vhost.Switch] • [HW.vhost.Switch_1] • [HW.switch.SwitchCPD_2] • [HW.switch.SwitchCPD_1] • [HW.switch.SwitchST] • [HW.switch.SwitchCCP2] • [HW.switch.SwitchBiblio] • [HW.other.Firewall_2] • [HW.other.Firewall_1] • [HW.Other.SwitchStack] • [HW.other.MiniFW_2] • [HW.other.MiniFW_1] • [SW.directory.DHCP_1] • [SW.directory.DHCP_2]	**Responsable**: • RSIS
Controles ENS: • mp.com.4	**Controles ISO/IEC 27001**: • 13.1.3

Tabla 55: Proyecto - Procedimiento de Segmentación de redes

Código: P-05-2020	**Nombre**: Procedimiento de control de acceso
Descripción: Asegurarse de que todos los usuarios o procesos disponen de un identificador único. Establecer un “periodo de retención” de las cuentas. Desarrollar un procedimiento de control de acceso detallando los mecanismos de identificación implementados. En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios.	
Situación específica del Ayuntamiento: Actualmente no existe un procedimiento detallado de control de acceso, por otro lado aunque el 99% de las cuentas del active directory, de los servicios de infraestructura,	

de las aplicaciones, etc. disponen de un identificador único aún quedan algunos usuarios genéricos utilizados por partidos de la oposición, usuarios de proveedores, etc. Uno de los objetivos de este proyecto es acabar con estas cuentas definitivamente. El Ayuntamiento tampoco cuenta con un periodo definido de retención de cuentas. Por otro lado para solucionar el problema de las cuentas de administrador locales se propone un randomificador de contraseñas locales, al menos se implantará en los equipos VDI de usuario desplegados, se utilizará Microsoft LAPS o una solución equivalente compatible con los sistemas operativos que dispone el Ayuntamiento.	
Activos involucrados: • [SW.Other.Padron] • [SW.Other.Eurocop] • [SW.Other.Lexnet] • [SW.Other.Siltra] • * [SW.Other.ZKSoft] • [SW.Other.GIS] • * [SW.Other.Reca] • * [SW.Other.Conta] • [SW.Other.AutoCAD19] • [SW.directory.DC_1] • [SW.directory.DC_2] • Usuarios administradores de los activos de infraestructura. • Usuarios administradores locales de los activos de infraestructura. • [S.saas.GestorExpedientes] • [S.cloud.SophosCentral] • [S.iaas.MailWeb] • [S.ca.Certs]	**Responsable**: • RSIS
Controles ENS: • op.acc.1	**Controles ISO/IEC 27001**: • 9.2.1 • 9.2.3 • 9.2.6

Tabla 56: Proyecto - Procedimiento de control de acceso

Código: P-06-2020	**Nombre**: Política de acceso a información
Descripción: Desarrollar e implementar una Política de acceso desarrollando un procedimiento de gestión de los derechos de acceso cumpliendo el requisito de “mínimo privilegio”. Realizar controles aleatorios de cumplimiento. Registrar estas acciones y sus resultados. Desarrollar un procedimiento de gestión de los derechos de acceso, que garantice que se asignan los mínimos privilegios y que son acordes a los establecidos para el control Requisitos de acceso [op.acc.2] y establecer tareas periódicas de revisión de los permisos otorgados. En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios.	

Situación específica del Ayuntamiento: En resumen documentar todos los procedimientos que ya se llevan a cabo en el Ayuntamiento de un modo sistemático pero sin reflejo en documentación oficial. Además se pueden automatizar algunos mecanismos como los de revisión de permisos otorgados, mediante el empleo de algún software. Por otro lado será necesario documentar la asignación de permisos para ello el Ayuntamiento puede adaptar su herramienta de ticketing (GLPI) de modo que se tramiten a través de él todas las solicitudes de acceso a información.	
Activos involucrados: • Todos los activos de la categoría [D] datos (excepto los excluidos por la evaluación de calidad). • [SW.directory.DC_1] • [SW.directory.DC_2]	**Responsable**: • RSIS • CSI
Controles ENS: • op.acc.2 • op.acc.4	**Controles ISO/IEC 27001**: • 9.1 • 9.2.2 • 9.2.3 • 9.2.5 • 9.2.6 • 9.4.1 • 9.4.4 • 12.6.2

Tabla 57: Proyecto - Política de acceso a información

Código: P-07-2020	**Nombre**: Instrucciones Técnicas de Configuración Segura
Descripción: Desarrollar Instrucciones Técnicas de configuración segura (bastionado) de los principales componentes del sistema: equipamiento (seguridad perimetral, electrónica de red, servidores físicos, servidores virtuales, bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.). Migrar los sistemas obsoletos (Windows XP, 2003 Server, etc.) a sistemas que dispongan de soporte de seguridad.	
Situación específica del Ayuntamiento: Si bien cuando se implantaron los equipos del Ayuntamiento se aplicaron una serie de best practices de fabricante, estas son muchas veces más orientadas al rendimiento que a la seguridad por lo que es necesario repasar toda esta configuración. Es interesante investigar si existen guías CCN-STIC de configuración segura específicas para los componentes del sistema, por ejemplo en el caso del Ayuntamiento se pueden seguir las guías 570A, 570B, 572 y 573 del CCN relativas exclusivamente al uso de MS Windows Server 2016. También es importante aplicar las Best Practices de seguridad del fabricante, para estos casos muchas veces lo mejor es consultar con el proveedor que lleve el mantenimiento para que nos asesore sobre cuales son estas buenas prácticas, investigar las que tenemos aplicadas y las que no y en caso de ser muy específicas dejar en manos de los técnicos del fabricante su implantación bajo nuestra observación con el fin de documentar el proceso. No quedan sistemas operativos obsoletos en el Ayuntamiento.	
Activos involucrados: • Todos los activos de tipo Hardware	**Responsable**: • RSIS

[HW] • [SW.OS.WIN12] • [SW.OS.WIN16] • [SW.OS.WIN10] • [SW.OS.CENT7] • [SW.dbms.SQL12] • [SW.hypervisor.Horizon7] • [SW.hypervisor.vCenterInfra] • [SW.hypervisor.vCenterVDI]	
Controles ENS: • op.exp.2 • op.exp.3 • mp.eq.3	**Controles ISO/IEC 27001**: • 6.2.1 (no es objetivo de este TFM) • 11.2.6 • 12.5.1

Tabla 58: Proyecto - Instrucciones Técnicas de Configuración Segura

Código: P-08-2020	**Nombre**: Gestión y Configuración de la Copias Seguridad
Descripción: Revisar el procedimiento de copias y asegurarse que las políticas implementadas respaldan toda la información, aplicaciones, logs, etc. En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el órgano competente de la política de copias de seguridad y de restauración. Mover físicamente la cabina de backup al edificio de Servicios Técnicos para minimizar riesgos.	
Situación específica del Ayuntamiento: El Ayuntamiento de la UOC cuenta con un potente y rápido sistema de backup que permite almacenar copias de seguridad de todas las máquinas virtuales de infraestructura y de todos los datos que tienen los usuarios de VDI en el escritorio para el intervalo de dos meses realizando una copia incremental por día y una completa por semana, no obstante el proceso no se ha documentado ni analizado y se puede optimizar configurando reglas específicas para logs, por ejemplo, es por ello que será necesario documentar y revisar que los procedimientos son correctos. Adicionalmente con el fin de minimizar riesgos de desastres naturales (por ejemplo), se puede llevar a cabo una acción relativamente sencilla que consistiría en mover la cabina de backup al edificio de Servicios Técnicos que se encuentra comunicado a 10G con el CPD para ello ya se cuenta con un rack acondicionado y con las conexiones necesarias en el switch de servicios técnicos, aunque faltaría dotar al cuarto donde reside el rack de elementos de climatización (actualmente el único switch que contiene no genera apenas calor), de aislamiento acústico (hay personas trabajando en el cuarto contiguo), control de acceso (al desplazar datos de carácter personal a este espacio), protección eléctrica (el SAI actual sería insuficiente y habría que poner uno mayor), etc. por lo tanto este proyecto se combinará con P-10-2020.	
Activos involucrados: • [SW.backup.Backup_1] • [SW.backup.Backup_2] • [L.building_ST]	**Responsable**: • RSIS

• [L.channel_fibraST] • [L.local_CPD] • [HW.data.CabinaBack]	
Controles ENS: • mp.info.9 • mp.if.3 • mp.if.4 • mp.if.5	**Controles ISO/IEC 27001**: • 12.3.1 • 11.1.4 • 11.2.1 • 11.2.2 • 11.2.3

Tabla 59: Proyecto - Gestión y Configuración de la Copias Seguridad

Código: P-09-2020	**Nombre**: Mejora de la Ciberseguridad
Descripción: Instalar la herramienta Lucia desarrollada por el CCN-CERT para la Gestión de Ciberincidentes. Completar la instalación con las sondas que ofrece (Internet y Red SARA). Instalar un IDS de red. Desarrollar un procedimiento integral de gestión de incidentes de seguridad con las obligaciones establecidas por el ENS y RGPD. En caso de servicios externalizados: completar con los procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos a las autoridades de control.	
Situación específica del Ayuntamiento: El Ayuntamiento actualmente no cuenta con IDS, ni con un procedimiento documentado de gestión de incidentes. La adquisición de la herramienta Lucia (al igual que Gloria) tiene una limitación y es que no debe ser instalada en máquinas virtuales por asuntos de latencia y configuración de las tarjetas de red virtuales, de modo que será necesaria la adquisición de un equipo workstation que instalaremos en el CPD conectado a los switches core con varias tarjetas de red y una capacidad de cómputo media-alta. Al poner la herramienta Lucia (o Gloria) en producción será necesario crear un documento de acuerdo de colaboración con nuestro CSIRT (el CCN).	
Activos involucrados: • Todos los activos de [COM] Red. • [HW.vhost.Switch] • [HW.vhost.Switch_1] • [HW.switch.SwitchCPD_2] • [HW.switch.SwitchCPD_1] • [HW.switch.SwitchST] • [HW.switch.SwitchCCP2] • [HW.switch.SwitchBiblio] • [HW.other.Firewall_2] • [HW.other.Firewall_1] • [HW.Other.SwitchStack] • [HW.other.MiniFW_2] • [HW.other.MiniFW_1]	**Responsable**: • RSEG

Controles ENS:	**Controles ISO/IEC 27001**:
• op.exp.7 • op.exp.9 • op.mon.1	• 6.1.3 • 6.1.4 • 13.1.2 • 16.1

Tabla 60: Proyecto - Mejora de la Ciberseguridad

Código: P-10-2020	**Nombre**: Mejora seguridad CPD
Descripción: Mejorar el mecanismo de acceso al CPD que permita identificar a las personas (incluido el acceso de terceros) extendiéndolo al nuevo CPD auxiliar donde almacenaremos la cabina de backup (P-08-2020). Desarrollar el procedimiento asociado. Revisar las medidas de acondicionamiento del CPD. Implantar un registro de entrada/salida de equipamiento al CPD. Desarrollar el procedimiento asociado.	
Situación específica del Ayuntamiento: Como hemos comentado en P-08-2020 tenemos que mover la cabina de backup a otro edificio, convirtiendo su ubicación en un pequeño CPD auxiliar por lo que será necesaria una adaptación completa de esta nueva ubicación para los nuevos requisitos. Para la revisión del acondicionamiento del CPD nos vamos a fijar sobretodo en el tapiado de una ventana que este dispone, se trata de un edificio antiguo (Casa Consistorial) no demasiado grande y en concreto en el cuarto del CPD existe una ventana, que si bien se encuentra bloqueada con planchas de acero, estas no se encuentran fijadas por lo que se debe inutilizar definitivamente la ventana. Otra revisión importante consistirá en el cambio y mejora del cuadro eléctrico que a pesar de llevar un mantenimiento y encontrarse en buenas condiciones no se encuentra aislado en exclusiva para el CPD lo que puede llevar a que salte el automático por algún accidente externo y que no se puede controlar desde el propio CPD, además el cuadro se encuentra al límite de sus capacidades y sería buen momento para ampliarlo a las nuevas necesidades. También se realizará una revisión del cableado extremo a extremo, no será necesario un saneamiento puesto que este se realizó hace relativamente poco. El CPD cuenta con un sistema doméstico de control de temperatura y suministro eléctrico, será conveniente cambiar este control por uno profesional que además agregue control de humedad e inundaciones. Finalmente tendremos que generar toda la documentación necesaria y desarrollar el procedimiento asociado. Este proyecto requerirá de trabajo en colaboración con el departamento de Urbanismo que lleva asuntos como obras (tapiado de la ventana), las emergencias, el sistema eléctrico del Ayuntamiento, etc.	
Activos involucrados: • Todos los activos pertenecientes a [AUX.CPD] • [L.local_CPD] • [L.building_ST]	**Responsable**: • RSIS

Controles ENS: • mp.if.2 • mp.if.3 • mp.if.7	**Controles ISO/IEC 27001**: • 11.1.2 • 11.1.4 • 11.2.1 • 11.2.2 • 11.2.3 • 11.2.5 • 11.2.6

Tabla 61: Proyecto - Mejora seguridad CPD

Código: P-11-2020	**Nombre**: Procedimiento de captura de registros de actividad
Descripción: Habilitar registros de las actividades de los usuarios realizadas sobre el Sistema, de forma que Indique quien las realiza, cuándo y sobre qué información. Desarrollar procedimiento asociado. Especialmente los de los administradores del sistema para monitorizar su actividad como medida compensatoria de op.acc.3. En caso de servicios externalizados: completar con procedimientos documentados de configuración de los registros de actividad de los usuarios a los servicios. Información/plataforma de visualización proporcionada por el órgano competente de los accesos de los administradores del sistema que soporta los servicios. Implantar un sistema automático de recolección de eventos de seguridad. Valorar que permita la correlación de los mismos (herramienta GLORIA CCN).	
Situación específica del Ayuntamiento: Si bien el Ayuntamiento ha habilitado a nivel de controlador de dominio los registros de las actividades, estos no abarcan las acciones de los usuarios dentro de las distintas herramientas software, además el proceso de recolección de evidencias es lento y costoso y no se encuentra documentado. Se implantará la herramienta GLORIA. Se hablará con todos los proveedores para conseguir documentación y acceso a los registros de actividades para cada herramienta software del Ayuntamiento.	
Activos involucrados: • Todos los activos pertenecientes a la categoría [D] Datos (quedan excluidos todos aquellos que no superaron la evaluación de calidad del dato)	**Responsable**: • RSIS
Controles ENS: • op.exp.8 • op.acc.3	**Controles ISO/IEC 27001**: • 6.1.2 • 12.4.1 • 12.4.3 • 12.4.4

Tabla 62: Proyecto - Procedimiento de captura de registros de actividad

Código: P-12-2020	**Nombre**: Puesta marcha de entornos de prueba/producción

Descripción:

Para servicios proporcionados directamente por el Ayuntamiento:

- Desarrollar e implantar un procedimiento donde se definan las pruebas, a realizar antes de la puesta en producción de las aplicaciones o bien solicitar al órgano competente en caso de que estos proporcionen este servicio.
- Realizar test de intrusión y análisis de vulnerabilidades, para todas las aplicaciones que ya están puestas en producción.
- Para los servicios y las aplicaciones web, además realizar pruebas de las amenazas que son propias de este entorno, realizar test de intrusión.
- Para los servicios web y aplicaciones web emplear "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.

En caso de servicios externalizados: recopilar los procedimientos documentados proporcionados por el órgano competente de coordinación con el Ayuntamiento para la realización de pruebas de aceptación y puesta en servicio. Informes resultados pruebas y plan de acción y los Informes proporcionados por el órgano competente con resultados de las inspecciones periódicas realizadas y plan de acción.

Situación específica del Ayuntamiento:

En el caso del Ayuntamiento es necesario definir el procedimiento de pruebas antes de la puesta en producción, actualmente se realiza un procedimiento definido por pliego para cada una de las implantaciones por separado, es necesario seguir una metodología unificada. Para el análisis de intrusión y vulnerabilidades se valorará el empleo de herramientas open source como por ejemplo Nessus, se contratará una empresa especializada para realizar los trabajos.

Activos involucrados:	**Responsable**:
• Todos los nuevos activos generados en el punto 5.2 de este TFM • Los test de intrusión y vulnerabilidades afectan a todos los activos de tipo software [SW] (excepto a los que no superaron la evaluación de calidad) • [S.saas.GestorExpedientes] • [S.iaas.MailWeb]	• RSIS
Controles ENS: • mp.sw.2 • mp.s.2	**Controles ISO/IEC 27001**: • 12.1.4 • 12.5.1 • 12.6.1 • 14.2.7 • 14.2.8 • 14.2.9 • 14.3.1 • 18.2.3

Tabla 63: Proyecto - Puesta marcha de entornos de prueba/producción

Código: P-13-2020	**Nombre**: Seguridad en mecanismos de autenticación

Descripción:

Identificar los mecanismos de autenticación de cada recurso y documentar como se encuentra implementado el doble factor de autenticación. Desarrollar el procedimiento

asociado.

Si se utilizan contraseñas: utilizar contraseñas seguras, definir una política de caducidad.

Inventariar los accesos remotos. Realizar un procedimiento que permita mantener este inventario, cómo se autorizan, etc. Realizar unas normas para los accesos remotos que regulen las condiciones en las cuales debe realizare este acceso. Revisar que los accesos remotos, se realizan, implementando doble factor de autenticación.

Configurar las directivas de acceso al dominio de forma que:

- Se establezca una limitación de intentos de acceso.
- Solo se muestre información, una vez validado en el dominio, por tanto, no se guardará la información del último usuario validado.
- Se informe al usuario de sus obligaciones.
- Se muestre la información sobre el último acceso con éxito y los posibles intentos de acceso.

En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el órgano competente de los mecanismos de autenticación de acceso a los servicios. Completar con procedimientos documentados proporcionados por el órgano competente de configuración de los requisitos del control: limitación de intentos de acceso, aviso de obligaciones, información sobre el último acceso.

Situación específica del Ayuntamiento:
Las plataformas cloud del Ayuntamiento cuentan con doble factor de autenticación aunque este no se encuentra documentado, por lo tanto el primer paso será realizar el documento del procedimiento de autenticación por usuario, no obstante el teletrabajo no dispone de segundo factor de autenticación, por lo que habrá que implantarlo.
Hay que documentar la política de contraseñas del Ayuntamiento, aunque esta ya sea correcta. Habrá que adaptar la herramienta GLPI para inventariar los accesos remotos.

Activos involucrados:	**Responsable**:
• Activos del grupo [SW.Clientes] • Activos del grupo [SW.Cloud] • [SW.directory.DC_1] • [SW.directory.DC_2] • [S.cloud.SophosCentral] • [S.saas.GestorExpedientes] • [S.iaas.MailWeb] • [SW.APP.VDISecurity] • [COM.other.Teletrabajo]	• RSIS
Controles ENS: • op.acc.5 • op.acc.6 • op.acc.7	**Controles ISO/IEC 27001**: • 9.1.2 • 9.2.1 • 9.2.2 • 9.2.4 • 9.2.6 • 9.3.1 • 9.4.2 • 9.4.3 • 10.1.1 • 13.1.1 • 13.1.2 • 18.1.5

Tabla 64: Proyecto - Seguridad en mecanismos de autenticación

5.2. Proyectos de mejora de la Calidad del Dato

A continuación exponemos los proyectos que nos permitirán deshacernos de aquellos activos que no pasaron la evaluación de calidad del dato y en los que priorizaremos su cambio a nuevos servicios seguros frente a la mejora de su propia seguridad.

<table>
<tr><td colspan="2">Código: C-01-2020 | Nombre: Servicios económicos del Ayuntamiento</td></tr>
<tr><td colspan="2">Descripción:
Tanto las aplicaciones de Recaudación como de Contabilidad no ofrecen Calidad de Dato, no ofrecen seguridad ENS, no ofrecen interoperabilidad ENI y no respetan el RGPD por lo que serán cambiadas.
Aunque los pliegos de prescripciones técnicas serán redactados los los expertos en la materia (tesorero e interventor), será necesario el asesoramiento por parte del RSEG y el RSIS para la redacción de la parte tecnológica.
Dentro del alcance del proyecto se tienen que contemplar conectores que permitan a ambas aplicaciones (Contabilidad y Recaudación) intercambiar información de un modo ágil ya sea entre ellas u obteniendo datos de la red Sara. También será necesario crear un canal de conexión con el gestor de expedientes con el fin de automatizar procesos como por ejemplo la apertura automática de oficio de un expediente siempre que se lleven a cabo procedimiento sancionadores ó al recibir facturas por FACE.
Si bien la solución a desarrollar puede ser local existen plataformas SaaS que ofrecen este servicio cumpliendo ENS con nivel alto, ENI, RGPD, ISO/IEC 27001, conexión propia con Red Sara y otros muchos estándares, y cuyo precio no dista mucho de una instalación local que cumpla todos estos requisitos, por lo se propondrá al Tesorero, Interventor y a la gerencia del Ayuntamiento el empleo de estas plataformas.
En la actualidad el software de Recaudación y Contabilidad se han especializado y será difícil que estos sean del mismo fabricante, por lo que es imprescindible reflejar en el pliego la interoperabilidad y el compromiso de trabajo colaborativo, además de redactarlo para que incluya dos lotes, uno para cada aplicación.</td></tr>
<tr><td>Activos sustituidos:
• [SW.Other.Conta]
• [SW.Other.Reca]
• [D.files.BD_Contabilidad]
• [D.files.BD_Recaudacion]
Activos involucrados
• [SW.dbms.SQL12]
• [S.saas.GestorExpedientes]
• [COM.vpn.RedSara]</td><td>Responsables:
• Tesorero
• Interventor
• RSEG y RSIS (asesoramiento técnico)</td></tr>
<tr><td>Controles ENS de implantación:
• mp.sw.2
• mp.s.2</td><td>Controles ISO/IEC 27001 de implantación:
• 12.1.4
• 12.5.1
• 12.6.1
• 14.2.7
• 14.2.8
• 14.2.9
• 14.3.1
• 18.2.3</td></tr>
</table>

Tabla 65: Proyecto - Servicios económicos del Ayuntamiento

<table>
<tr><td>Código: C-02-2020</td><td colspan="2">Nombre: Plataforma para el Empleado</td></tr>
<tr><td colspan="3">Descripción:
Tanto las aplicaciones de Intranet como de Fichajes no ofrecen Calidad de Dato, no ofrecen seguridad ENS, no ofrecen interoperabilidad ENI y no respetan el RGPD por lo que serán cambiadas.
Aunque los pliegos de prescripciones técnicas serán redactados los los expertos en la materia (resp. RRHH), será necesario el asesoramiento por parte del RSEG y el RSIS para la redacción de la parte tecnológica.
Se aprovecha la sustitución de este entorno para ganar en interoperabilidad y, dado el tamaño del Ayuntamiento, ofrecer una solución que integre fichajes, gestión de permisos, integración con nóminas, e integración con contabilidad.
Si bien la solución a desarrollar puede ser local existen plataformas SaaS que ofrecen este servicio cumpliendo ENS con nivel alto, ENI, RGPD, ISO/IEC 27001, conexión propia con Red Sara y otros muchos estándares, y cuyo precio no dista mucho de una instalación local que cumpla todos estos requisitos, por lo se propondrá al responsable de RRHH y a la gerencia del Ayuntamiento el empleo de estas plataformas.
Se adjunta como producto obtenido un pliego de prescripciones técnicas de ejemplo, este pliego no es definitivo y en concreto será necesario revisar la evaluación de las ofertas con el fin de adaptarlas a la situación real de seguridad que se pretende conseguir, no obstante puede servir de guía orientativa.
Producto obtenido “Ejemplo PPT.pdf”</td></tr>
<tr><td>Activos sustituidos:
• [SW.www.Intranet]
• [SW.Other.ZKSoft]
• [D.acl.BD_ZKSoft]
• [D.files.BD_Intranet]
Activos involucrados
• [SW.dbms.SQL12]
• [S.saas.GestorExpedientes]
• [SW.APP.Nominas]
• [D.files.BD_Nominas]
• [SW.Other.Siltra]
• [COM.vpn.RedSara]
• Activos de contabilidad obtenidos de C-01-2020</td><td colspan="2">Responsables:
• Resp. RRHH
• RSEG y RSIS (asesoramiento técnico)</td></tr>
<tr><td>Controles ENS de implantación:
• mp.sw.2
• mp.s.2</td><td colspan="2">Controles ISO/IEC 27001 de implantación:
• 12.1.4
• 12.5.1
• 12.6.1
• 14.2.7
• 14.2.8
• 14.2.9
• 14.3.1
• 18.2.3</td></tr>
</table>

Tabla 66: Proyecto - Plataforma para el Empleado

5.3. Cuantificación económica

Todos los importes se han calculado atendiendo a pliegos publicados en la Plataforma de Contratación del Estado (PCE) haciendo ponderaciones aproximadas

relativas a la población de los Ayuntamiento, al tamaño del sistema o a los servicios incluidos en las licitaciones, los precios son importes máximos que pueden ser a la baja, por ejemplo en el P-07-2020 se puede realizar una inspección previa que determine la cantidad de sistemas a incluir. Los proyectos no presentes en la siguiente tabla son asumidos en exclusiva por recursos internos del Ayuntamiento.

Código	**Recursos Ext. Necesarios**	**Referencia PCE**	**Presupuesto**
P-01-2020	Empresa de formación	2019/SER/14 Almendralejo	3.500 € IVA incluido
P-02-2020	Técnico Interino Informático *	Sueldo actual en el Ayuntamiento	35.000 € brutos/anuales
P-03-2020	Servicio de Pentesting	2018/CO_ASER/ 0038 Vitoria-Gasteiz	3.000 € IVA incluido **
P-07-2020	Servicio de Consultoría	2018/CO_ASER/ 0038 Vitoria-Gasteiz	3.500 € IVA incluido **
P-08-2020	Reinstalación de la cabina de backup	2019/2 suministro cabina Villaquilambre	2.000 € IVA incluido
P-09-2020	Implantar IDS de red	5.6/2018, Equipamiento de seguridad perimetral Agencia Valenciana Antifraud	10.000 € IVA incluido
P-10-2020	Reacondicionamiento CPD	14372019000003 OBRA NOU CPD Lloret de Mar	20.000 € IVA incluido
P-11-2020	Comprar Workstation para instalar GLORIA y LUCIA	Precio de mercado	1.500 € IVA incluido
P-12-2020	Servicio de consultoría en intrusión y vulnerabilidades	2018/CO_ASER/ 0038 Vitoria-Gasteiz	3.500 € IVA incluido **
C-01-2020	Renovación Servicios económicos del Ayuntamiento	2/2020 Jaén	40.000 € IVA incluido (anuales, años restantes de contrato se resta importe de instalación)
C-02-2020	Renovación Plataforma para el Empleado	Elaboración propia	8.000 € IVA incluido (anuales, años restantes de contrato se resta importe de instalación)
			TOTAL: 130.000 € IVA incluido

Tabla 67: Proyectos - Coste Económico

* Además de la redacción de los pliegos también ayudará al RSIS en los otros proyectos (p.e. en la segmentación de redes o en el desarrollo de documentación en los procesos donde el responsable sea el RSIS), el procedimiento óptimo será crear una bolsa de trabajo donde acudir siempre que se acumulen tareas.
** Estos proyectos se englobarán en un único pliego o contrato menor con el fin de ahorrar procedimientos de contratación, su total será la suma de los distintos proyectos.

Adicionalmente el Ayuntamiento deberá reservar una partida del 20% del importe total de la suma de los proyectos con el fin de poder hacer frente a posibles eventualidades o imprevistos.

5.4. Cuantificación temporal

En primer lugar vamos a indicar en qué parte del año es recomendable acometer los distintos proyectos para posteriormente definir las tareas de cada uno y relacionarlos en un diagrama de Gantt. La planificación deseada basada en nuestro plan de mejora de la seguridad sería la siguiente:

Código	Trimestre 1	Trimestre 2	Trimestre 3	Trimestre 4
P-01-2020	X	X		
P-02-2020	X	X		
P-03-2020	X			
P-04-2020		X		
P-05-2020	X	X		
P-06-2020	X	X		
P-07-2020		X	X	
P-08-2020	X			
P-09-2020	X	X		
P-10-2020		X		
P-11-2020		X	X	
P-12-2020			X	X
P-13-2020	X	X		
C-01-2020			X	X
C-02-2020			X	X

Tabla 68: Proyectos – Aproximación Planificación Trimestral

No obstante en una aproximación más realista vamos a crear un diagrama de Gantt que refleje las distintas tareas, por una parte llamaremos tareas de “Trabajo Interno” a todas aquellas que se realizan con recursos propios y por otro lado separaremos de los proyectos aquellas tareas que dependan de terceros. Por lo tanto las tareas se segregarán del siguiente modo:

- “P-01-2020-Trabajo Interno” y “P-01-2020-Formación”
- “P-02-2020-Contratación Personal” y “P-02-2020-Trabajo Interno”
- “P-03-2020-Trabajo Interno” y “P-03-2020-Pentesting”
- “P-04-2020-Trabajo Interno”
- “P-05-2020-Trabajo Interno”
- “P-06-2020-Trabajo Interno”
- “P-07-2020-Trabajo Interno” y “P-07-2020-Consultoría”
- “P-08-2020-Trabajo Interno” y “P-08-2020-Reinstalar Cabina”
- “P-09-2020-Trabajo Interno” y “P-09-2020-Implantar IDS”
- “P-10-2020-Reacondicionar CPD” y “P-10-2020-Trabajo Interno”
- “P-11-2020-Comprar Workstation” y “P-11-2020-Trabajo Interno”
- “P-12-2020-Trabajo Interno” y “P-12-2020-Vulnerabilidades”
- “C-01-2020-Contratación” y “C-01-2020-Implantación”
- “C-02-2020-Contratación” y “C-02-2020-Implantación”
- “P-(03,07,10,12)-2020-Contratación”: esta tarea especial es la encargada de llevar a cabo los procesos de contratación de los servicios necesarios para llevar a cabo los proyectos P-03-2020, P-07-2020, P-10-2020 y P-12-2020

Se respeta el mes de Agosto como mes de vacaciones para el personal. En rojo tenemos las tareas realizadas por el CSI, en verde las que son en exclusiva del RSEG, en amarillo las del técnico informático auxiliar que se contrata en “P-02-2020-Contratación Personal” y en azul las que realiza el RSIS:

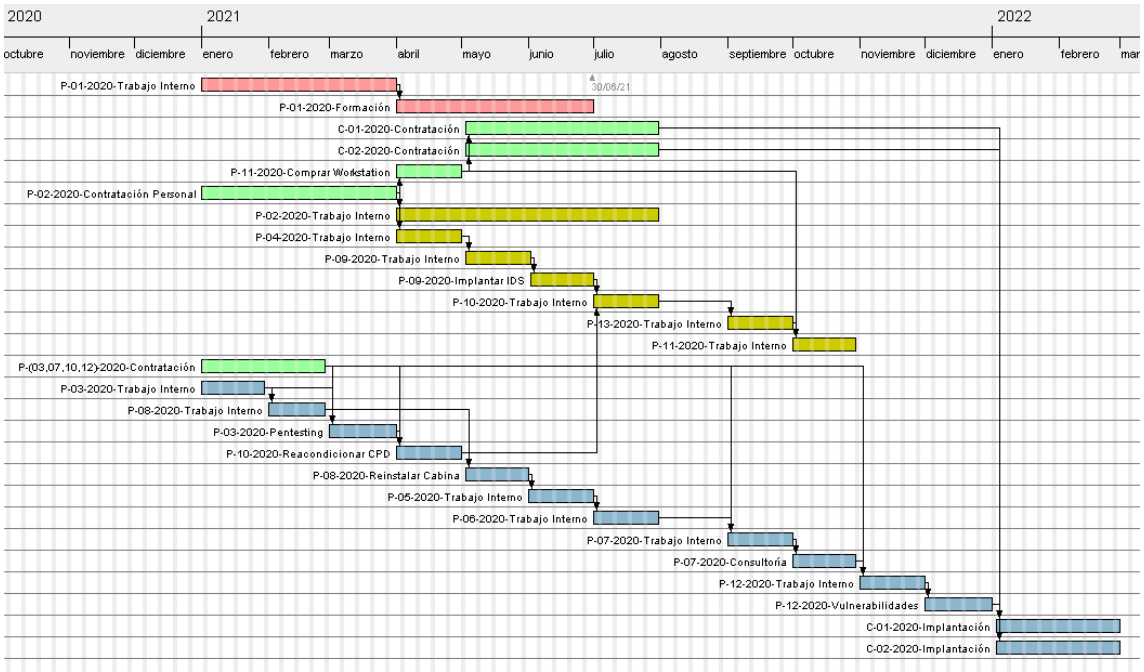

Figura 11- Diagrama Gantt Proyectos Mejora Seguridad

En una aproximación más realista como la de la figura anterior podemos observar como es complicado que finalmente los proyectos se lleven a cabo en los trimestres ideales, e incluso los proyectos de la calidad del dato queden fuera del alcance del año natural dado que es necesario cumplir antes con P-12-2020 “Puesta en marcha de entornos de prueba/producción”.

Notas adicionales:

- La contratación del técnico auxiliar debe contemplarse hasta final de año con el fin de poder paliar posibles eventualidades o imprevistos, las tareas que se le han asignado son las más “sencillas” de modo que su no conocimiento inicial del entorno no repercuta en exceso en sus labores, será necesario contratarlo atendiendo al perfil de las labores que va a realizar.
- No han sido reflejadas las tareas de licitación para los proyectos C-01-2020 y C-02-2020 dado que no implican a personal responsable de seguridad, aunque se entiende que los periodos de publicación, licitación y adjudicación transcurren entre septiembre y diciembre.
- Los proyectos de terceros P-03-2020-Pentesting, P-07-2020-Consultoría, P-10-2020-Reacondicionar CPD y P-12-2020-Vulnerabilidades pueden ser tramitados por contratos menores al ser de única aplicación (no se repiten) y entrar dentro de los importes de los contratos menores (P-03-2020 entra dentro del contrato menor de obra).
- P-01-2020 sí que se considera un gasto anual repetitivo por lo que sería recomendable realizar una licitación simplificada durante el transcurso de la tarea P-01-2020-Trabajos Internos.
- Por importe P-08-2020-Reinstalar Cabina se puede realizar por hoja de pedido como gasto corriente.

5.5. Impacto de los proyectos sobre la seguridad

A continuación mostramos una serie de gráficos donde se puede observar en azul la mejora sobre el riesgo acumulado una vez aplicados los proyectos sobre el estado actual de la seguridad en rojo:

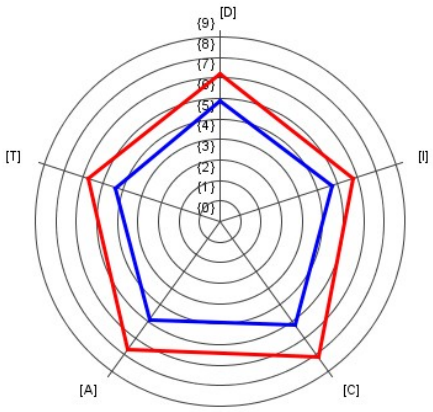

Figura 13 - Mejora de la seguridad sobre la [D]isponibilidad, [T]razabilidad, [C]onfidencialidad, [I]ntegridad, y [A]utenticidad

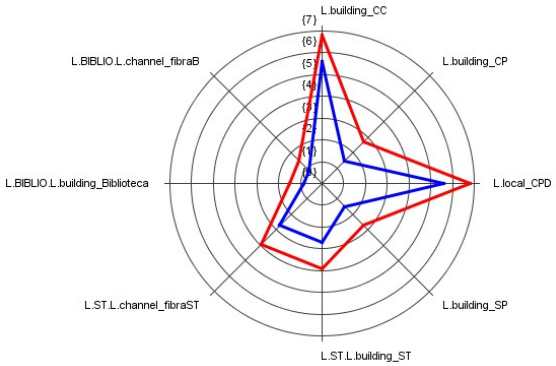

Figura 12 - Mejora de la seguridad sobre Instalaciones

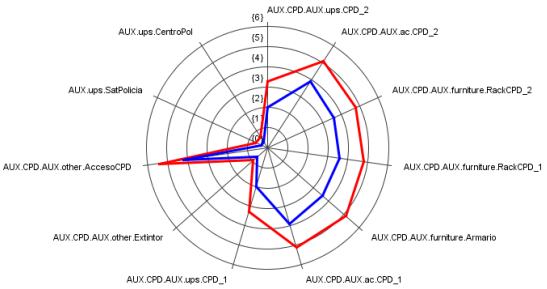

Figura 14 - Mejora de la seguridad sobre Equipamiento Auxiliar

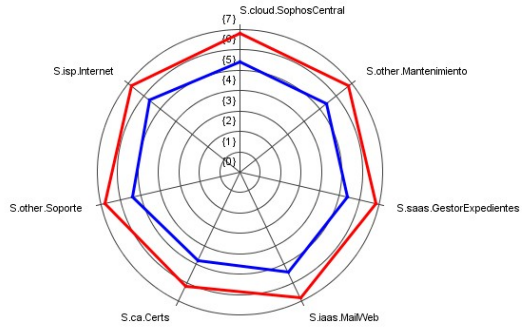

Figura 15 - Mejora de la seguridad sobre Servicios

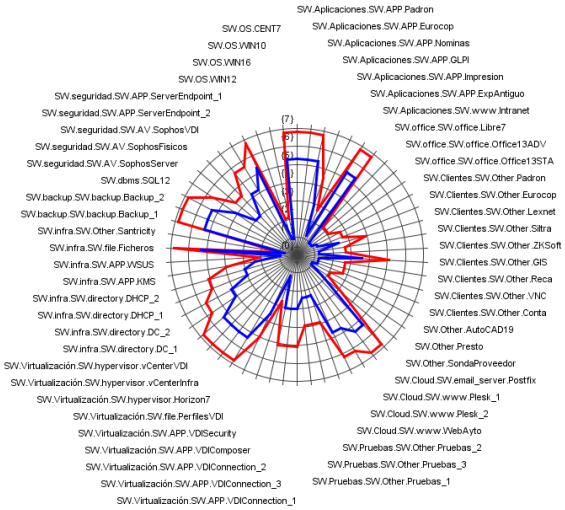

Figura 16 - Mejora de la seguridad sobre Software

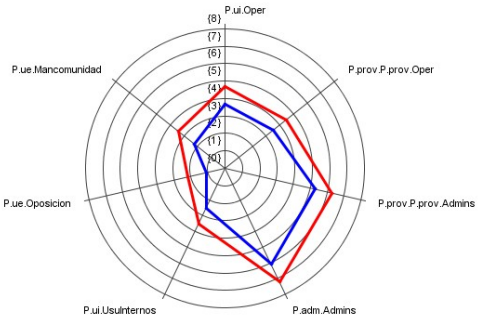

Figura 17 - Mejora de la seguridad sobre Personal

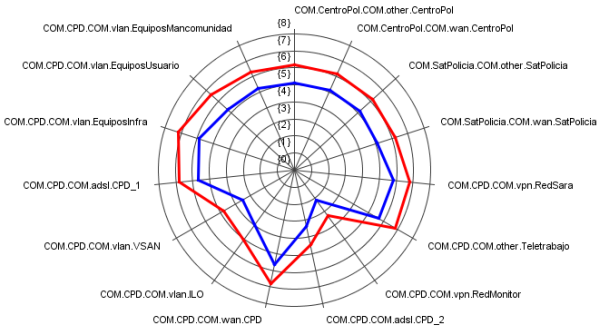

Figura 18 - Mejora de la seguridad sobre Red

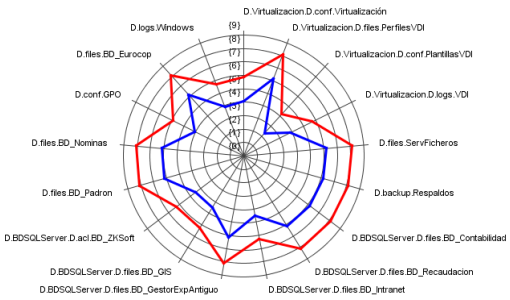

Figura 19 - Mejora de la seguridad sobre Datos

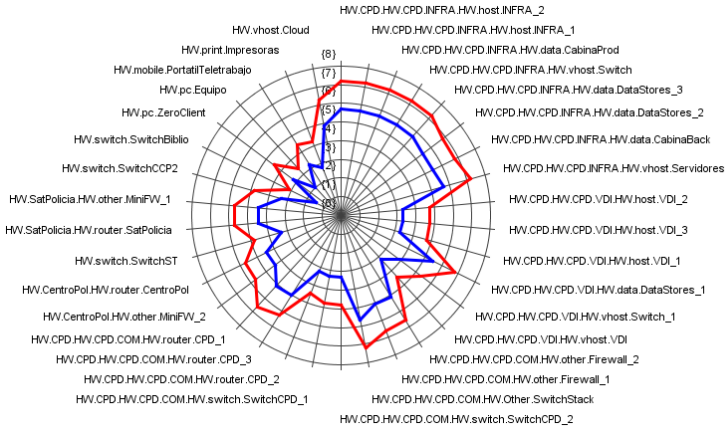

Figura 20 - Mejora de la seguridad sobre Hardware

5.6. Futuros proyectos de adecuación al ENS

Los siguientes proyectos quedan fuera del primer acercamiento (primera fase) al ENS pero deberán ser abordados en los siguientes años/ciclos.

Código: Org-01-XX	**Nombre**: Procedimientos de Seguridad
Descripción: Desarrollar procedimientos operativos que recojan las principales tareas sobre el sistema. Indicando los responsables de su realización y cómo identificar y reportar comportamientos anómalos. Integrar en un Sistema de Gestión de Seguridad de la Información que de soporte al cumplimiento del ENS. (SGSIENS).	
Responsables: RSEG y RSIS	
Controles ENS de implantación: • org.3	**Controles ISO/IEC 27001**: • 12.1.1 • 13.2.1 • 16.1.1 • 16.1.2 • 16.1.3 • 18.1.2 • 18.2.3

Tabla 69: Proyectos ENS - Procedimientos de Seguridad

Código: Org-02-XX	**Nombre**: Procesos de Autorización
Descripción: Implantar y documentar un proceso de autorización para la introducción de elementos en el sistema: instalaciones, equipos, aplicaciones, medios de comunicación, utilización de soportes, portátiles, móviles, etc. y servicios de terceros.	
Responsable: RSIS	
Controles ENS de implantación: • org.4	**Controles ISO/IEC 27001**: • 6.1.2 • 6.2.1 • 8.3.1 • 11.2.5 • 11.2.6 • 12.5.1 • 12.6.2 • 13.1.1 • 13.1.2 • 14.2.4 • 15.1.1

Tabla 70: Proyectos ENS - Procesos de Autorización

Código: Pl-01-XX	**Nombre**: Arquitectura de Seguridad
Descripción: Recopilar, organizar, completar y mantener actualizada documentación sobre: áreas y puntos de acceso, del sistema, líneas de defensa, identificación y autenticación, controles técnicos, relaciones con terceros, para que formen parte del SGSIENS. En caso de servicios externalizados: completar con la documentación proporcionada por el órgano competente sobre las comunicaciones con el Ayuntamiento, y con otros sistemas interconectados comunicaciones con el Ayuntamiento, y con otros sistemas interconectados.	

Responsable: RSIS	
Controles ENS de implantación: • op.pl.2	**Controles ISO/IEC 27001**: • 5.1.2 • 8.1.1 • 11.1.5 • 11.1.6 • 13.1.1 • 14.2.5

Tabla 71: Proyectos ENS - Arquitectura de Seguridad

Código: Pl-02-XX	**Nombre**: Adquisición de Nuevos Componentes
Descripción: Implantar un procedimiento que analice los riesgos, evalúe la necesidad de requisitos antes de la adquisición de nuevos componentes. Registrar estas acciones y sus resultados.	
Responsable: RSIS	
Controles ENS de implantación: • op.pl.3	**Controles ISO/IEC 27001**: • 14.1.1

Tabla 72: Proyectos ENS - Adquisición de nuevos componentes

Código: Pl-03-XX	**Nombre**: Dimensionamiento y gestión de la capacidad
Descripción: Implantar un procedimiento para la realización de un estudio de estos parámetros antes de la entrada en producción de nuevos elementos. En caso de servicios externalizados: completar con la documentación regular proporcionada por el órgano competente sobre los recursos disponibles y consumidos.	
Responsable: RSIS	
Controles ENS de implantación: • op.pl.4	**Controles ISO/IEC 27001**: • 12.1.3

Tabla 73: Proyectos ENS - Dimensionamiento y gestión de la capacidad

Código: Acc-01-XX	**Nombre**: Segregación de funciones y tareas
Descripción: Elaborar un procedimiento documento de asignación de tareas con indicación de las tareas críticas y la incompatibilidad entre estas. – Medida compensatoria en caso de que sea necesario incluido en incluido en medidas priorizadas.	
Responsable: RSIS	
Controles ENS de implantación: • op.acc.3	**Controles ISO/IEC 27001**: • 6.1.2

Tabla 74: Proyectos ENS - Segregación de funciones y tareas

Código: Exp-01-XX	**Nombre**: Procedimiento de Inventario de Activos
Descripción: Desarrollar un procedimiento que describa la forma en la que se gestionan los activos. Realizar un inventario de software (se recomienda utilizar una herramienta que realice un inventario de activos hardware, software de forma automática).	
Responsable: RSIS	
Controles ENS de implantación: • op.exp.1	**Controles ISO/IEC 27001**: • 8.1.1 • 8.1.2

Tabla 75: Proyectos ENS - Procedimiento de inventario de activos

Código: Exp-02-XX	**Nombre**: Procedimiento de Mantenimiento
Descripción: Documentar todas las acciones de mantenimiento (físico y lógico). Registrar estas acciones y sus resultados. Desarrollar un procedimiento para analizar, prioridad la aplicación de actualizaciones de seguridad, parches, mejoras, etc. En caso de servicios externalizados: completar con procedimientos documentados de coordinación con el Ayuntamiento para realizar acciones de mantenimiento sobre el sistema.	
Responsable: RSIS	
Controles ENS de implantación: • op.exp.4	**Controles ISO/IEC 27001**: • 11.2.4 • 12.6.1

Tabla 76: Proyectos ENS - Procedimiento de Mantenimiento

Código: Exp-03-XX	**Nombre**: Gestión de cambios externalizada
Descripción: En caso de servicios externalizados: recopilar la información aportada por el la órgano competente de coordinación con el Ayuntamiento para realizar cambios sobre el sistema que soporta los servicios.	
Responsable: RSIS	
Controles ENS de implantación: • op.exp.5	**Controles ISO/IEC 27001**: • 12.1.2 • 14.2.4 • 14.2.2 • 15.2.2 • 14.2.3

Tabla 77: Proyectos ENS - Gestión de cambios externalizada

Código: Exp-04-XX	**Nombre**: Protección de las claves criptográficas
Descripción: Documentar las medias de seguridad implementadas para garantizar la protección de las claves criptográficas durante todo su ciclo de vida. Para sistemas de categoría media se asegurará la utilización de programas evaluados o dispositivos criptográficos evaluados que empleen algoritmos acreditados por el CCN.	

En caso de servicios externalizados: completar con procedimientos documentados de protección de las claves criptográficas del Ayuntamiento que se encuentren alojadas en el sistema que soporta los servicios.	
Responsable: RSIS	
Controles ENS de implantación: • op.exp.11	**Controles ISO/IEC 27001**: • 10.1.2

Tabla 78: Proyectos ENS - Protección de las claves criptográficas

Código: Mon-01-XX	**Nombre**: Sistema de métricas
Descripción: Realizar un procedimiento que establezca los indicadores, métrica asociada y designación de responsables para su recopilación de los elementos para dar respuesta a la encuesta INES (re-querido por el artículo 35).	
Responsable: RSIS	
Controles ENS de implantación: • op.mon.2	**Controles ISO/IEC 27001**: -

Tabla 79: Proyectos ENS – Sistema de métricas

Código: If-01-XX	**Nombre**: Áreas separadas y control de acceso
Descripción: Realizar un procedimiento que contengan un inventario de todas las áreas donde se concentra el sistema de información y que detalle los mecanismos implementados en cada caso para controlar el acceso a las mismas y las autorizaciones pertinentes en caso de que sea necesario.	
Responsable: RSIS	
Controles ENS de implantación: • mp.if.1	**Controles ISO/ IEC 27001**: • 11.1.1 • 11.1.2 • 11.1.3 • 11.1.5 • 11.1.6 • 11.2.1

Tabla 80: Proyectos ENS - Áreas separadas y control de accesos

Código: If-02-XX	**Nombre**: Energía eléctrica
Descripción: Documentar las medidas implementadas para garantizar el suministro eléctrico en el CPD. En caso de que sea de aplicación describir las medidas adicionales implementadas (SAI, grupo electrónico, la forma y cuando entran en funcionamiento, pruebas de contingencia realizadas para determinar los cálculos de tiempo).	
Responsable: RSIS	
Controles ENS de implantación: • mp.if.4	**Controles ISO/ IEC 27001**: • 11.2.2

Tabla 81: Proyectos ENS - Energía eléctrica

Código: If-03-XX	**Nombre**: Protección frente a incendios
Descripción: Desarrollar un procedimiento que recoja la forma en la cual se protegen los locales conforme a la normativa industrial, la ubicación de los carteles, extintores, materiales no inflamables, etc. Los controles periódicos realizados, etc. Mantener de forma centralizada toda la documentación relacionada Mantener de forma centralizada toda la documentación relacionada).	
Responsable: RSIS	
Controles ENS de implantación: • mp.if.5	**Controles ISO/ IEC 27001**: • 11.1.4 • 11.2.1

Tabla 82: Proyectos ENS - Protección frente a incendios

Código: Per-01-XX	**Nombre**: Deberes y obligaciones de personal
Descripción: Desarrollar un procedimiento de gestión de personal que describa la forma en la cual se trasladan los deberes al personal propio o de terceros.	
Responsable: CSI	
Controles ENS de implantación: • mp.per.2	**Controles ISO/ IEC 27001**: • 7.1.2 • 7.3.1 • 7.2.1 • 8.1.4 • 7.2.3 • 13.2.4

Tabla 83: Proyectos ENS - Deberes y obligaciones de personal

Código: Com-01-XX	**Nombre**: Perímetro Seguro
Descripción: Documentar la seguridad perimetral y las excepciones implementadas en los firewalls. Proceso de autorización y que describa la separación de flujos implementada.	
Responsable: RSIS	
Controles ENS de implantación: • mp.com.1	**Controles ISO/ IEC 27001**: • 13.1.2

Tabla 84: Proyectos ENS - Perímetro seguro

Código: Com-02-XX	**Nombre**: Protección de la confidencialidad
Descripción: Realizar un procedimiento que describa la forma en la cual se protege la confidencialidad de la información cuanto esta discurre por redes fuera del propio dominio de seguridad. En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre los mecanismos de cifrado implementados en las comunicaciones.	
Responsable: RSIS	

Controles ENS de implantación:	**Controles ISO/ IEC 27001**:
• mp.com.2	• 10.1.1 • 13.1.1 • 13.1.2 • 14.1.2 • 18.1.5

Tabla 85: Proyectos ENS - Protección de la confidencialidad

Código: Com-03-XX	**Nombre**: Protección de la autenticidad y de la integridad
Descripción: Realizar un procedimiento/norma que establezca la necesidad de utilizar redes privadas virtuales para garantizar la autenticidad y la integridad de la información antes de su intercambio. En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre los mecanismos implementados para proteger la autenticidad y de la integridad.	
Responsable: RSIS	
Controles ENS de implantación: • mp.com.3	**Controles ISO/ IEC 27001**: • 10.1.1 • 13.1.1 • 13.1.2 • 13.2.1 • 14.1.2

Tabla 86: Proyectos ENS - Protección de la autenticidad y de la integridad

Código: Si-01-XX	**Nombre**: Etiquetado
Descripción: Desarrollar un procedimiento para el etiquetado de soportes extraíbles conforme a la calificación de la información que contienen. Difundir al personal afectado.	
Responsable: RSIS	
Controles ENS de implantación: • mp.si.1	**Controles ISO/ IEC 27001**: • 8.2.2 • 8.3.1

Tabla 87: Proyectos ENS – Etiquetado

Código: Si-02-XX	**Nombre**: Custodia
Descripción: Desarrollar un procedimiento para la custodia de soportes de información. Difundir al personal afectado.	
Responsable: RSIS	
Controles ENS de implantación: • mp.si.3	**Controles ISO/ IEC 27001**: • 8.3.1

Tabla 88: Proyectos ENS - Custodia

Código: Si-03-XX	**Nombre**: Transporte
Descripción: Desarrollar un procedimiento que describa las medidas de seguridad a aplicar durante el transporte a los soportes de información. Difundir al personal afectado.	
Responsable: RSIS	
Controles ENS de implantación: • mp.si.4	**Controles ISO/ IEC 27001**: • 8.3.3 • 11.2.5

Tabla 89: Proyectos ENS – Transporte

Código: Si-04-XX	**Nombre**: Borrado y destrucción
Descripción: Desarrollar un procedimiento que describa el procedimiento a seguir para el borrado y destrucción en función del soporte. Elaborar instrucción técnica de borrado y de destrucción.	
Responsable: RSIS	
Controles ENS de implantación: • mp.si.5	**Controles ISO/ IEC 27001**: • 8.3.2 • 11.2.7

Tabla 90: Proyectos ENS - Borrado y destrucción

Código: Info-01-XX	**Nombre**: Datos de carácter personal
Descripción: Desarrollar las acciones de seguridad necesarias para llevar a cabo la implantación de la normativa de protección de datos (RAT, designación DPD, Análisis de Riegos RGPD, Evaluación de Impacto, contratos de encargado del tratamiento, alinear medidas de seguridad con las del ENS). En caso de servicios externalizados: recopilar documentos /plataformas online, proporcionados por el órgano competente, con evidencias de cumplimiento de la normativa de protección de datos.	
Responsable: CSI	
Controles ENS de implantación: • mp.info.1	**Controles ISO/ IEC 27001**: • 18.1.4

Tabla 91: Proyectos ENS - Datos de carácter personal

Código: Info-02-XX	**Nombre**: Calificación de la Información
Descripción: Desarrollar e implantar un procedimiento de calificación de la información. Elaborar procedimientos que definan la forma que hay que tratar la documentación en consideración al nivel de seguridad requerido.	
Responsable: CSI	
Controles ENS de implantación: • mp.info.2	**Controles ISO/ IEC 27001**: • 8.1.2 • 8.2

Tabla 92: Proyectos ENS - Calificación de la información

Código: Info-03-XX	**Nombre**: Firma electrónica
Descripción: Desarrollar, aprobar y dar publicidad a la Política de Firma Electrónica. Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de firma electrónica. En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre las medidas de protección de la firma implementadas.	
Responsable: CSI	
Controles ENS de implantación: • mp.info.4	**Controles ISO/ IEC 27001**: • 10.1.1 • 14.1.3 • 18.1.5

Tabla 93: Proyectos ENS - Firma electrónica

Código: Info-04-XX	**Nombre**: Sellos de tiempo
Descripción: Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de sello electrónico. En caso de servicios externalizados: recopilar documentos proporcionados por el órgano competente con información sobre las medidas de seguridad implementadas para proteger el sello de tiempo.	
Responsable: CSI	
Controles ENS de implantación: • mp.info.5	**Controles ISO/ IEC 27001**: -

Tabla 94: Proyectos ENS - Sellos de tiempo

Código: Info-05-XX	**Nombre**: Limpieza de documentos
Descripción: Desarrollar e Implantar un procedimiento donde se establezca la forma en la cual se ha de proceder para la limpieza de los documentos electrónicos.	
Responsable: CSI	
Controles ENS de implantación: • mp.info.6	**Controles ISO/ IEC 27001**: -

Tabla 95: Proyectos ENS - Limpieza de documentos

Código: S-01-XX	**Nombre**: Protección del correo electrónico
Descripción: Desarrollar un procedimiento que describa la forma en la cual se protege el correo.	
Responsable: RSIS	
Controles ENS de implantación: • mp.s.1	**Controles ISO/ IEC 27001**: • 7.2.2 • 13.2.3

Tabla 96: Proyectos ENS - Protección del correo electrónico

Código: S-02-XX	**Nombre**: Protección frente a la denegación de servicio
Descripción: Documentar las medidas de seguridad implementadas. Realizar el procedimiento asociado.	
Responsable: RSIS	
Controles ENS de implantación: • mp.s.8	**Controles ISO/ IEC 27001**: -

Tabla 97: Proyectos ENS - Protección frente a la denegación de servicio

Código: SW-01-XX	**Nombre**: Desarrollo Software por Terceros
Descripción: Para servicios proporcionados directamente por el Ayuntamiento: • En caso de que se encargue a terceros desarrollo de software, solicitar que se utilicen metodologías de desarrollo seguro y que satisfagan los requisitos necesarios para cumplir con el ENS. • En caso de adquirir software para instalación en modo local solicitar la conformidad con el ENS, en categoría MEDIA, y los requisitos adicionales requeridos por el "Abstract- Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local".	
Responsable: CSI	
Controles ENS de implantación: • mp.sw.1	**Controles ISO/ IEC 27001**: • 6.1.5 • 9.4.5 • 12.1.4 • 14.2.1 • 14.2.2 • 14.2.5 • 14.2.6 • 14.2.7 • 14.2.8 • 14.3.1

Tabla 98: Proyectos ENS - Desarrollo Software por Terceros

5.7. Otros Proyectos de adecuación a ISO/IEC 27001:2013

Finalmente nos queda agregar proyectos no contemplados en los controles ENS pero que sí se contemplan en los controles de ISO/IEC 27001:2013:

Código: ISO-01-XX	**Nombre**: Procedimiento de Auditorías de los SI
Descripción: Acordar los requerimientos de las auditorías. Documentar el procedimiento de la auditoría estableciendo responsabilidades. Establecer mecanismos para evitar que durante el proceso de auditoría se produzcan amenazas como fallos técnicos, acciones no autorizadas, compromiso de la información o de las funciones y en general pérdida de servicios esenciales.	

Responsable: RSEG	
Controles ENS de implantación: -	**Controles ISO/ IEC 27001**: • 12.7.1

Tabla 99: Proyectos ISO - Procedimiento de Auditorías de los SI

Código: ISO-02-XX	**Nombre**: Protección de los registros de la organización
Descripción: Establecer y documentar medidas para evitar la pérdida, destrucción, falsificación o el acceso no autorizado a los registros del sistema de información.	
Responsable: RSIS	
Controles ENS de implantación: -	**Controles ISO/ IEC 27001**: • 18.1.3

Tabla 100: Proyectos ISO - Protección de los registros de la organización

Código: ISO-03-XX	**Nombre**: Revisión independiente de los SI
Descripción: Licitar y planificar labores externas independientes donde se aborde la revisión de la documentación existente, los objetivos de control, los controles, los procesos y los procedimientos para la seguridad de la información.	
Responsable: RSEG	
Controles ENS de implantación: -	**Controles ISO/ IEC 27001**: • 18.2.1

Tabla 101: Proyectos ISO - Revisión independiente de los SI

Código: ISO-04-XX	**Nombre**: Protección de la información de registro
Descripción: Los registros se protegerán contra accesos de lectura no autorizados, contra borrado y modificación no autorizados. Se creará un mecanismo para conceder acceso únicamente de lectura. Se guardarán en dispositivos de una sola escritura. Se realizarán copias de seguridad y estas garantizarán el mismo nivel de seguridad. En caso de fallo del sistema, se garantizará la disponibilidad de los datos registrados hasta ese momento.	
Responsable: RSIS	
Controles ENS de implantación: -	**Controles ISO/ IEC 27001**: • 12.4.2

Tabla 102: Proyectos ISO - Protección de la información de registro

Código: ISO-05-XX	**Nombre**: Continuidad de la seguridad de la información
Descripción: Realización de un análisis de impacto (BIA). Los requisitos de seguridad	

de la información se trasladarán a los elementos dispuestos para garantizar la continuidad. Se desarrollará un Plan de Recuperación de Desastres (DRP). Se establecerá el procedimiento de actualización de inventario Los medios alternativos (hardware, software, etc.) estarán sujetos a las mismas garantías de protección que los medios habituales. Se establecerá procedimiento de verificación para garantizar que los elementos de continuidad de negocio satisfacen los requisitos de seguridad de la información. Los incidentes detectados durante pruebas, ejercicios o activaciones de los procesos de continuidad se analizarán como si se hubieran producido sobre el sistema base.	
Responsable: RSEG	
Controles ENS de implantación: -	**Controles ISO/ IEC 27001**: • 17.1.1 • 17.1.2 • 17.1.3

Tabla 103: Proyectos ISO - Continuidad de la seguridad de la información

Todos estos proyectos incluidos en nuestro plan de mejora de la seguridad se referenciarán durante la Auditoría de Cumplimiento para poder ayudar al Ayuntamiento a priorizar las acciones correctivas del nuevo ciclo de implantación del ENS e ISO/IEC 27001:2013.

6. Auditoría de Cumplimiento

Llegados a este punto estamos cercanos de finalizar nuestro Plan Director para el Ayuntamiento de la UOC, para ello hemos redactado toda la documentación necesaria, hemos llevado a cabo una identificación de los activos con su análisis de riesgos correspondiente y hemos propuesto una serie de proyectos de mejora en la seguridad. El siguiente paso natural es observar cómo han ayudado estos proyectos a mejorar la seguridad de la información mediante la realización de una nueva evaluación de la madurez y exponer los hallazgos encontrados.

6.1. Evaluación de los controles y la madurez

En primer lugar determinaremos cómo vamos a proceder con la auditoría:

- ISO/IEC 27002:2013. Se analizarán un total de 114 controles o salvaguardas, descritas en la norma organizadas en 14 dominios y 35 objetivos de control.

- ENS. Se analizarán los controles o salvaguardas de los distintos marcos organizativos (org, op, mp) atendiendo a la categoría media del sistema.

Estas salvaguardas actúan reduciendo el riesgo según distintos aspectos como son generalmente la formalización de las prácticas mediante documentos escritos o aprobados, la política de personal, las solicitudes técnicas (software, hardware o comunicaciones) y la seguridad física.

Los dominios de control principales a analizar serán: política de seguridad, organización de la seguridad de la información, gestión de activos, seguridad de los recursos humanos, seguridad física y ambiental, gestión de comunicaciones y operaciones, control de acceso, adquisición-desarrollo-mantenimiento de Sistemas de Información, gestión de incidentes, gestión de continuidad de negocio y cumplimiento.

Para valorar cada uno de los controles utilizaremos la siguiente tabla basada en el Modelo de Madurez de la Capacidad (CMM):

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial /Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.

			Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones.

Tabla 104: Modelo de Madurez de la Capacidad

Finalmente nos apoyaremos en la herramienta PILAR del CCN para presentar los resultados, utilizamos tanto su versión para el ENS como su versión para ISO/IEC 27000, no obstante con el fin de obtener resultados consistentes en los informes se modifica la plantilla de reporte de PILAR para el cumplimiento de ISO/IEC 27000 de modo que los gráficos sean radiales en lugar de barras tal y como viene configurado por defecto (**producto obtenido plantilla ISO 27000:2013 para PILAR con gráficos radiales: patterns_27000_2013.xml**) [42].

Se analizar en primer lugar el cumplimiento de la normativa ENS y a continuación la ISO/IEC 27000:2013, hay que hacer notar que los controles ISO no se corresponden al completo con los controles ENS, un control ISO puede encontrarse distribuido a través de varios controles ENS. Debido a esta casuística y con el fin de simplificar la auditoría de cumplimiento, a la hora de evaluar ISO/IEC 27000:2013 comprobaremos si los controles se encuentran en los proyectos prioritarios, en caso afirmativo subiremos el nivel CMM a L3 para ese control en el software PILAR, posteriormente repasaremos si en los proyectos futuros (apartados 5.6 y 5.7 de este TFM) es necesario volver a implementar estos controles, en caso afirmativo bajaremos el nivel CMM de ese control a L2 si este se encontrase en nivel L3 y no se encontrase ya en L3 en la evaluación preliminar realizada en el punto 2.4.3 de este TFM. Este modo es una simplificación del método real donde en la evaluación de cada control serían necesarias la adopción de una serie de medidas que se valorarían durante la

auditoría real, por ejemplo el control 11.1.1 ISO/IEC 27000:2013 se compone de las siguientes salvaguardas:

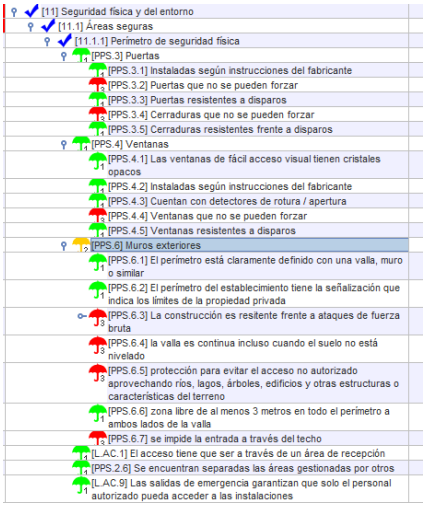

Figura 21 - Ejemplo salvaguardas completas 11.1.1 ISO/IEC 27000:2013

Todos estos puntos de control se comprobarían en un entorno real, nosotros trabajaremos con un entorno "simulado". No sucede el mismo problema al contrario por la forma de trabajar que hemos tomado aproximándonos desde el ENS hacía ISO/IEC 27000:2013, de habernos aproximado desde ISO/IEC 27000:2013 hacia el ENS se hubiesen tenido que repasar los controles ENS, en nuestro caso tratándose de una administración pública es mejor la aproximación realizada.

6.2. Evaluación del nivel de cumplimiento de las normativas

6.2.1. Esquema Nacional de Seguridad

A continuación presentamos los resultados para el Esquema Nacional de seguridad atendiendo a los distintos Marcos, en las tablas presentadas podremos observar las columnas "Anterior" que representan el estado inicial del sistema, "Actual" que representan el estado del sistema durante la realización de la auditoría, en los gráficos podremos observar en rojo la situación "Anterior", en azul la situación "Actual" y se añade en verde la recomendación de cumplimiento hecha por PILAR.

Todos los resultados están disponibles en formato PILAR en el **producto obtenido: Evaluación madurez actual ENS.mgr**

6.2.1.1. Marco organizativo

control	Anterior	Actual
[org] Marco organizativo	L0-L1	L1-L3
[org.1] Política de Seguridad	L0	L3
[org.2] Normativa de seguridad	L0	L3
[org.3] Procedimientos de seguridad	L1	L1
[org.4] Proceso de autorización	L1	L1

Tabla 105: Auditoría ENS - Marco organizativo

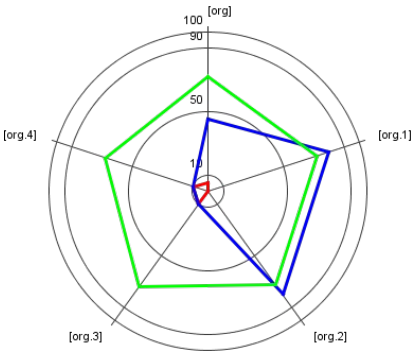

Figura 22 - Auditoría ENS - Marco organizativo

6.2.1.2. Marco operacional

6.2.1.2.1. Planificación

control	Anterior	Actual
[op] Marco operacional	L1-L3	L1-L3
[op.pl] Planificación	L1-L2	L1-L3
[op.pl.1] Análisis de riesgos	L1	L3
[op.pl.2] Arquitectura de seguridad	L1	L1
[op.pl.3] Adquisición de nuevos componentes	L2	L2
[op.pl.4] Dimensionamiento / Gestión de capacidades	L2	L2
[op.pl.5] Componentes certificados	n.a.	n.a.

Tabla 106: Auditoría ENS - Planificación

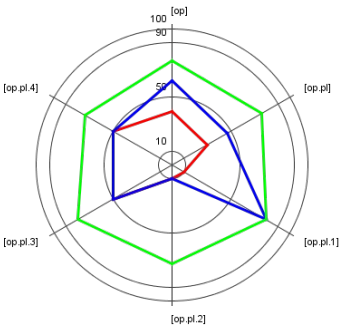

Figura 23 - Auditoría ENS - Planificación

6.2.1.2.2 Control de Acceso

control	Anterior	Actual
[op] Marco operacional	L1-L3	L1-L3
[op.acc] Control de acceso	L1-L2	L1-L3
[op.acc.1] Identificación	L2	L3
[op.acc.2] Requisitos de acceso	L2	L3
[op.acc.3] Segregación de funciones y tareas	L1	L3
[op.acc.4] Proceso de gestión de derechos de acceso	L2	L3
[op.acc.5] Mecanismo de autenticación	L2	L3
[op.acc.6] Acceso local (local logon)	L2	L3
[op.acc.7] Acceso remoto (remote login)	L1-L2	L1-L3

Tabla 107: Auditoría ENS - Control de Acceso

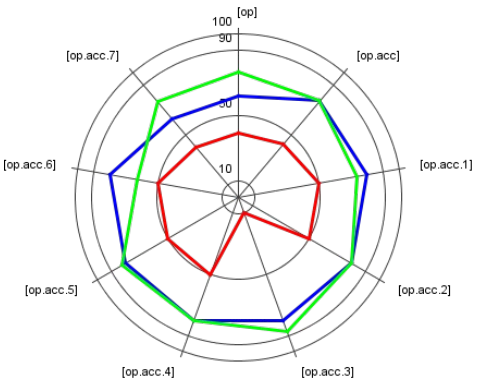

Figura 24 - Auditoría ENS - Control de Acceso

6.2.1.2.3. Explotación

control	Anterior	Actual
[op] Marco operacional	L1-L3	L1-L3
[op.exp] Explotación	L1-L2	L1-L3

[op.exp.1] Inventario de activos	L1	L1
[op.exp.2] Configuración de seguridad	L2	L3
[op.exp.3] Gestión de la configuración	L1	L3
[op.exp.4] Mantenimiento	L2	L2
[op.exp.5] Gestión de cambios	n.a.	n.a.
[op.exp.6] Protección frente a código dañino	L2	L3
[op.exp.7] Gestión de incidentes	L1	L3
[op.exp.8] Registro de la actividad de los usuarios	L1	L3
[op.exp.9] Registro de la gestión de incidentes	L2	L3
[op.exp.10] Protección de los registros de actividad	n.a.	n.a.
[op.exp.11] Protección de claves criptográficas	L1	L1

Tabla 108: Auditoría ENS – Explotación

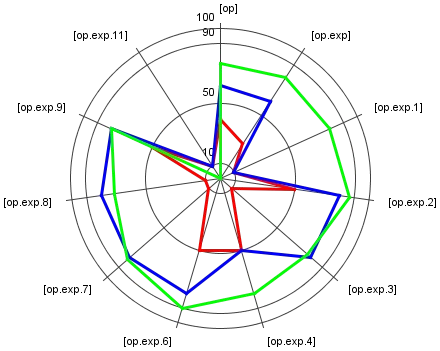

Figura 25 - Auditoría ENS - Explotación

6.2.1.2.4. Servicios Externos

control	**Anterior**	**Actual**
[op] Marco operacional	L1-L3	L1-L3
[op.ext] Servicios externos	L2	L3
[op.ext.1] Contratación y acuerdos de nivel de servicio	L2	L3
[op.ext.2] Gestión diaria	L2	L3
[op.ext.9] Medios alternativos	n.a.	n.a.

Tabla 109: Auditoría ENS - Servicios Externos

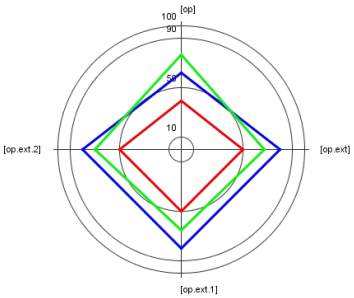

Figura 26 - Auditoría ENS - Servicios Externos

6.2.1.2.5. Continuidad del servicio

No aplica. En ISO/ IEC 27001:2013 tendría que aplicar.

6.2.1.2.6. Monitorización del Sistema

control	Anterior	Actual
[op] Marco operacional	L1-L3	L1-L3
[op.mon] Monitorización del sistema	L1-L3	L1-L3
[op.mon.1] Detección de intrusión	L3	L3
[op.mon.2] Sistema de métricas	L1	L1

Tabla 110: Auditoría ENS - Monitorización del Sistema

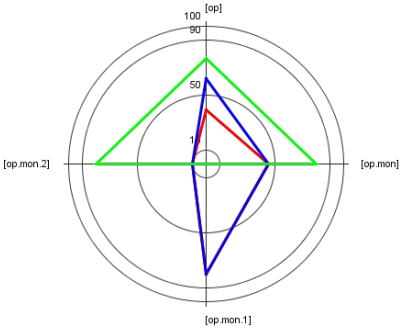

Figura 27 - Auditoría ENS - Monitorización del Sistema

6.2.1.3. Medidas de protección

6.2.1.3.1. Protección de las instalaciones e infraestructuras

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.if] Protección de las instalaciones e infraestructuras	L1-L2	L1-L3
[mp.if.1] Áreas separadas y con control de acceso	L1	L1
[mp.if.2] Identificación de las personas	L1	L3
[mp.if.3] Acondicionamiento de los locales	L2	L3
[mp.if.4] Energía eléctrica	L2	L3
[mp.if.5] Protección frente a incendios	L2	L3
[mp.if.6] Protección frente a inundaciones	n.a.	n.a.
[mp.if.7] Registro de entrada y salida de equipamiento	L2	L3
[mp.if.9] Instalaciones alternativas	n.a.	n.a.

Tabla 111: Auditoría ENS - Protección de las instalaciones e infraestructuras

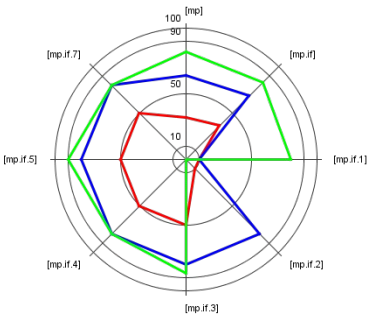

Figura 28 - Auditoría ENS - Protección de las instalaciones e infraestructuras

6.2.1.3.2. Gestión del Personal

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.per] Gestión del personal	L1-L3	L3
[mp.per.1] Caracterización del puesto de trabajo	n.a.	n.a.
[mp.per.2] Deberes y obligaciones	L3	L3
[mp.per.3] Concienciación	L1	L3
[mp.per.4] Formación	L1	L3
[mp.per.9] Personal alternativo	n.a.	n.a.

Tabla 112: Auditoría ENS - Gestión del Personal

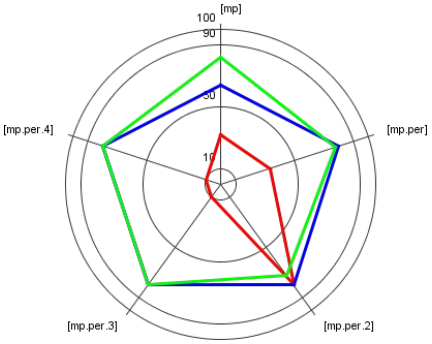

Figura 29 - Auditoría ENS - Gestión del Personal

6.2.1.3.3. Protección de los Equipos

Control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.eq] Protección de los equipos	L1-L2	L3
[mp.eq.1] Puesto de trabajo despejado	L1	L3
[mp.eq.2] Bloqueo del puesto de trabajo	L2	L3

Control	Anterior	Actual
[mp.eq.3] Protección de equipos portátiles	L1	L3
[mp.eq.9] Medios alternativos	n.a.	n.a.

Tabla 113: Auditoría ENS - Protección de los Equipos

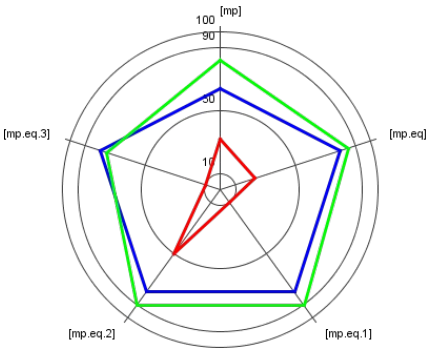

Figura 30 - Auditoría ENS - Protección de los Equipos

6.2.1.3.4. Protección de las comunicaciones

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.com] Protección de las comunicaciones	L1-L3	L1-L3
[mp.com.1] Perímetro seguro	L3	L3
[mp.com.2] Protección de la confidencialidad	n.a.	n.a.
[mp.com.3] Protección de la autenticidad y de la integridad	L1	L1
[mp.com.4] Segregación de redes	L2	L3
[mp.com.9] Medios alternativos	n.a.	n.a.

Tabla 114: Auditoría ENS - Protección de las comunicaciones

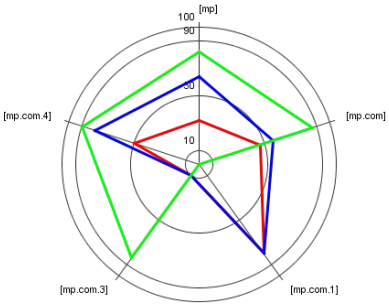

Figura 31 - Auditoría ENS - Protección de las comunicaciones

6.2.1.3.5. Protección de los soportes de información

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.si] Protección de los soportes de información	L1	L3
[mp.si.1] Etiquetado	L1	L3
[mp.si.2] Criptografía	n.a.	n.a.
[mp.si.3] Custodia	L1	L3
[mp.si.4] Transporte	L1	L3
[mp.si.5] Borrado y destrucción	L1	L3

Tabla 115: Auditoría ENS - Protección de los soportes de información

Para este gráfico la herramienta PILAR no muestra el objetivo de cumplimiento del ENS esto es debido a su aplicación dependiendo de si los soportes contienen información o no. Se debe entender como recomendación a todos los valores el aplicado a “mp” Medidas de protección, excepto en Criptografía que no aplica a nuestro sistema por ser de nivel medio.

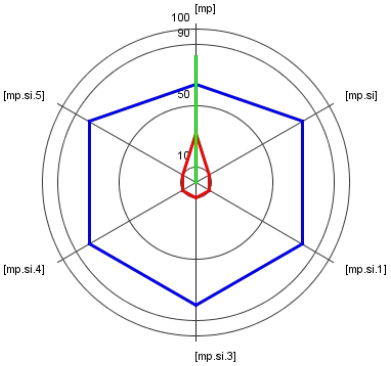

Figura 32 - Auditoría ENS - Protección de los soportes de información

6.2.1.3.6. Protección de las aplicaciones informáticas

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.sw] Protección de las aplicaciones informáticas (SW)	L2	L2-L3
[mp.sw.1] Desarrollo de aplicaciones	L2	L2
[mp.sw.2] Aceptación y puesta en servicio	L2	L3

Tabla 116: Auditoría ENS - Protección de las aplicaciones informáticas

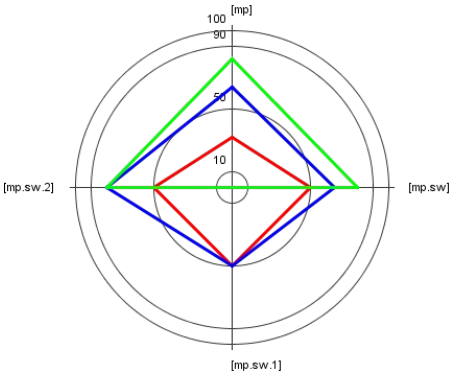

Figura 33 - Auditoría ENS - Protección de las aplicaciones informáticas

6.2.1.3.7. Protección de la información

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.info] Protección de la información	L1-L2	L1-L3
[mp.info.1] Datos de carácter personal	L1	L1
[mp.info.2] Calificación de la información	L1	L1
[mp.info.3] Cifrado de la información	n.a.	n.a.
[mp.info.4] Firma electrónica	L1	L1
[mp.info.5] Sellos de tiempo	L1	L1
[mp.info.6] Limpieza de documentos	L1	L3
[mp.info.9] Copias de seguridad (backup)	L2	L3

Tabla 117: Auditoría ENS - Protección de la información

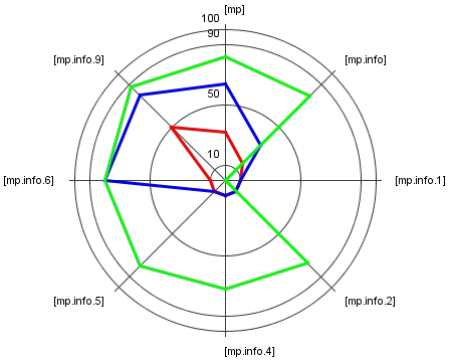

Figura 34 - Auditoría ENS - Protección de la información

6.2.1.3.8. Protección de los servicios

control	Anterior	Actual
[mp] Medidas de protección	L1-L3	L1-L3
[mp.s] Protección de los servicios	L1-L2	L1-L3
[mp.s.1] Protección del correo electrónico (e-mail)	L1	L1
[mp.s.2] Protección de servicios y aplicaciones web	L2	L3
[mp.s.8] Protección frente a la denegación de servicio	L2	L2
[mp.s.9] Medios alternativos	n.a.	n.a.

Tabla 118: Auditoría ENS - Protección de los servicios

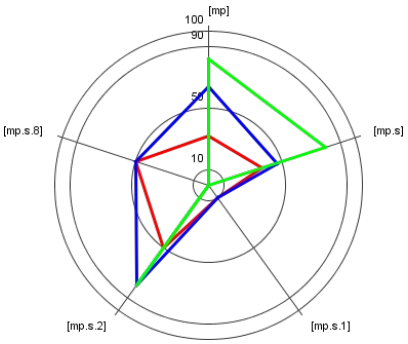

Figura 35 - Auditoría ENS - Protección de los servicios

6.2.2. ISO/IEC 27002:2013

A continuación presentamos los resultados para ISO/IEC 27002:2013 atendiendo a los distintos dominios, en las tablas presentadas podremos observar las columnas “Anterior” que representan el estado inicial del sistema, “Actual” que representan el estado del sistema durante la realización de la auditoría, en los gráficos podremos observar en rojo la situación “Anterior”, en azul la situación “Actual” y se añade en verde la recomendación de cumplimiento hecha por PILAR.

En nuestra declaración de aplicabilidad (**ver producto obtenido: Declaración de Aplicabilidad.pdf**) existen varios controles ISO/IEC 27002:2013 que decidimos marcarlos como no aplicables, esto se realiza bajo una perspectiva del ENS para dar consistencia al documento y porque estamos acercándonos a ISO/IEC 27001:2013 desde el proceso de certificación del ENS. Esta declaración de aplicabilidad no sería correcta si el proceso lo realizásemos al contrario y estuviésemos en primer lugar tomando el camino de la certificación ISO/IEC 27001:2013 dado que este estándar, aunque tiene elementos en común, no busca los mismos objetivos que el ENS. Aclarado este punto y teniendo delante de nosotros el encargo de realizar una Auditoría de Cumplimiento, se toma la decisión de incluir estos controles “no aplicables” dentro de la auditoría (a excepción de los ya descartados justificadamente en el análisis diferencial inicial del punto 2.4.3 de este TFM) puesto que de lo contrario no se trataría de una Auditoría de Cumplimiento para ISO/IEC 27002:2013 si no de la repetición de la Auditoría de Cumplimiento para el ENS pero bajo la perspectiva de los controles de ISO/IEC 27002:2013, algo que carece de sentido.

Todos los resultados están disponibles en formato PILAR en el **producto obtenido: Evaluación madurez actual ISO 27001.mgr**

6.2.2.1. Políticas de seguridad

control	Anterior	Actual
[5] Políticas de seguridad de la información	L1-L2	L2-L3
[5.1] Directrices de gestión de la seguridad de la información	L1-L2	L2-L3
[5.1.1] Políticas para la seguridad de la información	L2	L3
[5.1.2] Revisión de las políticas para la seguridad de la información	L1	L2

Tabla 119: Auditoría ISO 27002 - Políticas de Seguridad

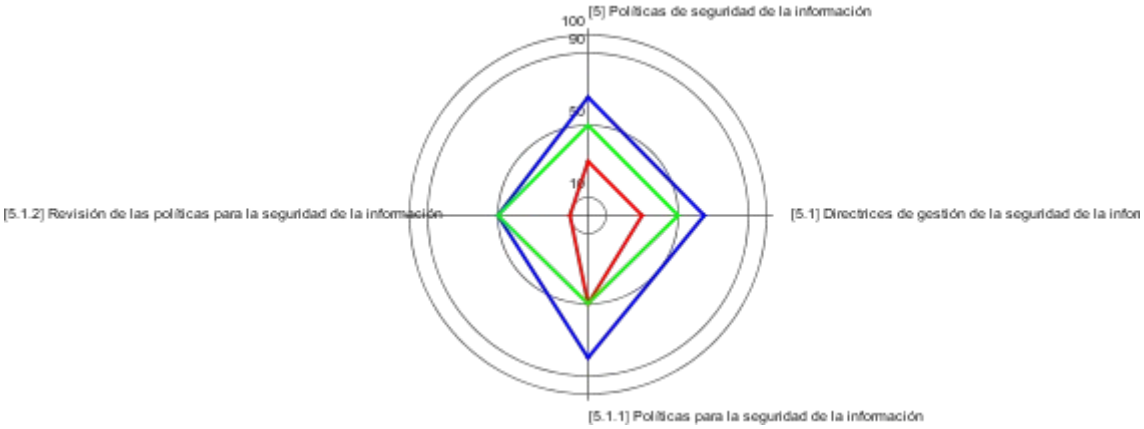

Figura 36 - Auditoría ISO 27002 - Políticas de Seguridad

6.2.2.2. Organización de la seguridad de la información

control	Anterior	Actual
[6] Organización de la seguridad de la información	L1	L1-L3
[6.1] Organización interna	L1	L1-L3
[6.1.1] Roles y responsabilidades en seguridad de la información	L1	L3
[6.1.2] Separación de tareas	L1	L2
[6.1.3] Contacto con las autoridades	L1	L3
[6.1.4] Contacto con grupos de interés especial	L1	L3
[6.1.5] Seguridad de la información en la gestión de proyectos	L1	L1
[6.2] Los dispositivos móviles y el teletrabajo	L1	L2-L3
[6.2.1] Política de dispositivos móviles	L1	L2
[6.2.2] Teletrabajo	L1	L3

Tabla 120: Auditoría ISO 27002 - Organización de la seguridad de la información

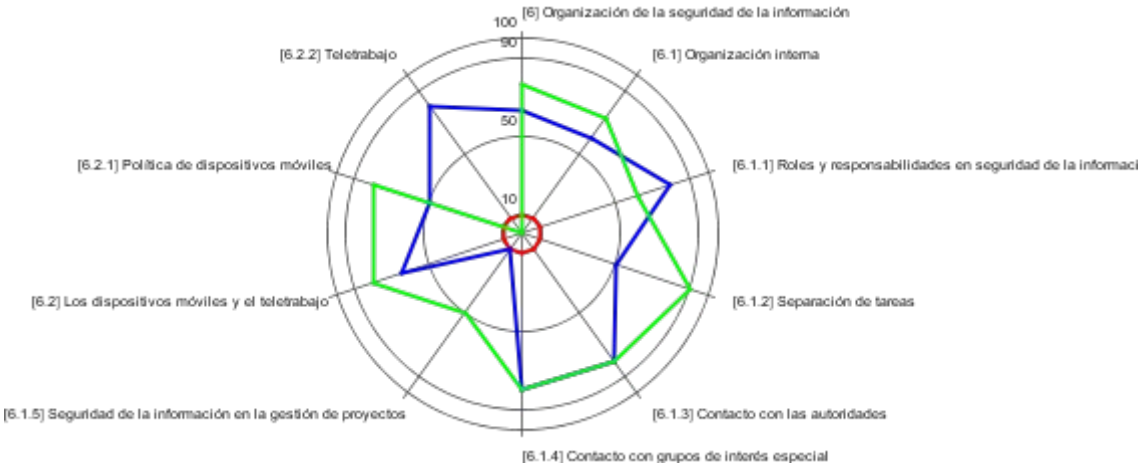

Figura 37 - Auditoría ISO 27002 - Organización de la seguridad de la información

6.2.2.3. Seguridad relativa a los recursos humanos

control	Anterior	Actual
[7] Seguridad relativa a los recursos humanos	L1-L3	L1-L3
[7.1] Antes del empleo	L3	L3
[7.1.1] Investigación de antecedentes	L3	L3
[7.1.2] Términos y condiciones del empleo	L3	L3
[7.2] Durante el empleo	L1-L3	L1-L3
[7.2.1] Responsabilidades de gestión	L1	L1
[7.2.2] Concienciación, educación y capacitación en seguridad de la información	L1	L2
[7.2.3] Proceso disciplinario	L3	L3
[7.3] Finalización del empleo o cambio en el puesto de trabajo	L1	L1
[7.3.1] Responsabilidades ante la finalización o cambio	L1	L1

Tabla 121: Auditoría ISO 27002 - Seguridad relativa a los recursos humanos

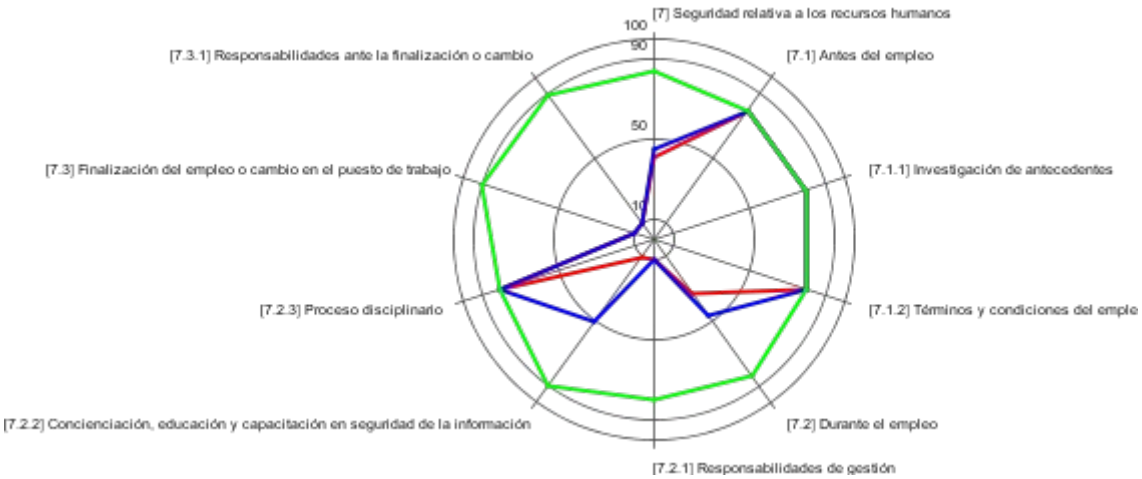

Figura 38 - Auditoría ISO 27002 - Seguridad relativa a los recursos humanos

6.2.2.4. Gestión de activos

control	Anterior	Actual
[8] Gestión de activos	L1	L1-L3
[8.1] Responsabilidad sobre los activos	L1	L1-L3
[8.1.1] Inventario de activos	L1	L1
[8.1.2] Propiedad de los activos	L1	L1
[8.1.3] Uso aceptable de los activos	L1	L3
[8.1.4] Devolución de activos	L1	L1
[8.2] Clasificación de la información	L1	L1
[8.2.1] Clasificación de la información	L1	L1
[8.2.2] Etiquetado de la información	L1	L1
[8.2.3] Manipulado de la información	L1	L1
[8.3] Manipulación de los soportes	L1	L1-L2
[8.3.1] Gestión de soportes extraíbles	L1	L2
[8.3.2] Eliminación de soportes	L1	L1
[8.3.3] Soportes físicos en tránsito	L1	L2

Tabla 122: Auditoría ISO 27002 - Gestión de activos

Figura 39 - Auditoría ISO 27002 - Gestión de activos

6.2.2.5. Control de acceso

control	Anterior	Actual
[9] Control de acceso	L2-L3	_-L3
[9.1] Requisitos de negocio para el control de acceso	L2	L3
[9.1.1] Política de control de acceso	L2	L3
[9.1.2] Acceso a las redes y a los servicios de red	L2	L3
[9.2] Gestión de acceso de usuario	L2	L3
[9.2.1] Registro y baja de usuario	L2	L3
[9.2.2] Provision de acceso de usuario	L2	L3
[9.2.3] Gestión de privilegios de acceso	L2	L3

control	Anterior	Actual
[9.2.4] Gestión de la información secreta de autenticación de los usuarios	L2	L3
[9.2.5] Revisión de los derechos de acceso de usuario	L2	L3
[9.2.6] Retirada o reasignación de los derechos de acceso	L2	L3
[9.3] Responsabilidades del usuario	L2	L3
[9.3.1] Uso de la información secreta de autenticación	L2	L3
[9.4] Control de acceso a sistemas y aplicaciones	L3	_-L3
[9.4.1] Restricción del acceso a la información	L3	L3
[9.4.2] Procedimientos seguros de inicio de sesión	L3	L3
[9.4.3] Sistema de gestión de contraseñas	L3	L3
[9.4.4] Uso de utilidades con privilegios del sistema	L3	L3
[9.4.5] Control de acceso al código fuente de los programas	n.a.	

Tabla 123: Auditoría ISO 27002 - Control de acceso

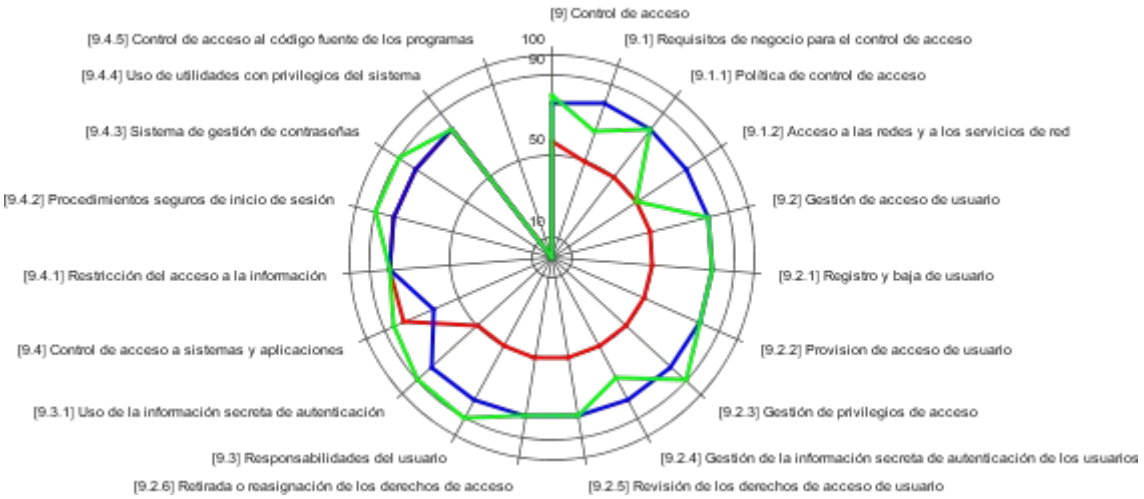

Figura 40 - Auditoría ISO 27002 - Control de acceso.

NOTA: en el gráfico se puede observar un pequeño bug en el punto 9.4 donde la línea roja no debería sobrepasar a la azul, los datos son correctos, no se ha encontrado modo de solucionar el problema.

6.2.2.6. Criptografía

control	Anterior	Actual
[10] Criptografía	L1	L1-L2
[10.1] Controles criptográficos	L1	L1-L2
[10.1.1] Política de uso de los controles criptográficos	L1	L2
[10.1.2] Gestión de claves	L1	L1

Tabla 124: Auditoría ISO 27002 - Criptografía

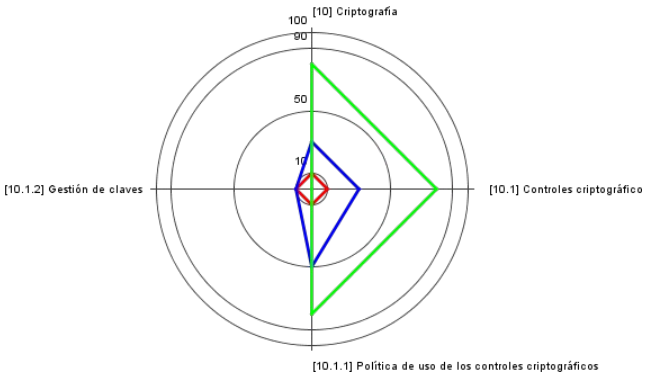

Figura 41 - Auditoría ISO 27002 - Criptografía

6.2.2.7. Seguridad física y del entorno

control	Anterior	Actual
[11] Seguridad física y del entorno	L1-L3	L1-L3
[11.1] Áreas seguras	L1-L3	L1-L3
[11.1.1] Perímetro de seguridad física	L3	L3
[11.1.2] Controles físicos de entrada	L1	L2
[11.1.3] Seguridad de oficinas, despachos y recursos	L1	L1
[11.1.4] Protección contra las amenazas externas y ambientales	L2	L2
[11.1.5] El trabajo en áreas seguras	L1	L1
[11.1.6] Áreas de carga y descarga	L1	L1
[11.2] Seguridad de los equipos	L1-L3	L2-L3
[11.2.1] Emplazamiento y protección de equipos	L2	L2
[11.2.2] Instalaciones de suministro	L2	L2
[11.2.3] Seguridad del cableado	L1	L3
[11.2.4] Mantenimiento de los equipos	L3	L3
[11.2.5] Retirada de materiales propiedad de la empresa	L2	L2
[11.2.6] Seguridad de los equipos fuera de las instalaciones	L1	L2
[11.2.7] Reutilización o eliminación segura de equipos	L3	L3
[11.2.8] Equipo de usuario desatendido	L2	L3
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia	L1	L3

Tabla 125: Auditoría ISO 27002 - Seguridad física y del entorno

Figura 42 - Auditoría ISO 27002 - Seguridad física y del entorno

6.2.2.8. Seguridad de las operaciones

control	Anterior	Actual
[12] Seguridad de las operaciones	L1-L3	L1-L3
[12.1] Procedimientos y responsabilidades operacionales	L1-L2	L1-L3
[12.1.1] Documentación de los procedimientos de operación	L1	L1
[12.1.2] Gestión de cambios	L1	L1
[12.1.3] Gestión de capacidades	L2	L2
[12.1.4] Separación de los recursos de desarrollo, prueba y operación	L2	L3
[12.2] Protección contra el software malicioso (malware)	L3	L3
[12.2.1] Controles contra el código malicioso	L3	L3
[12.3] Copias de seguridad	L2	L3
[12.3.1] Copias de seguridad de la información	L2	L3
[12.4] Registros y supervisión	L2	L2-L3
[12.4.1] Registro de eventos	L2	L3
[12.4.2] Protección de la información de registro	L2	L2
[12.4.3] Registros de administración y operación	L2	L3
[12.4.4] Sincronización del reloj	L2	L3
[12.5] Control del software en explotación	L2	L2
[12.5.1] Instalación del software en explotación	L2	L2
[12.6] Gestión de la vulnerabilidad técnica	L1-L2	L2
[12.6.1] Gestión de las vulnerabilidades técnicas	L1	L2
[12.6.2] Restricción en la instalación de software	L2	L2
[12.7] Consideraciones sore la auditoría de sistemas de información	L1	L1
[12.7.1] Controles de auditoría de sistemas de información	L1	L1

Tabla 126: Auditoría ISO 27002 - Seguridad de las operaciones

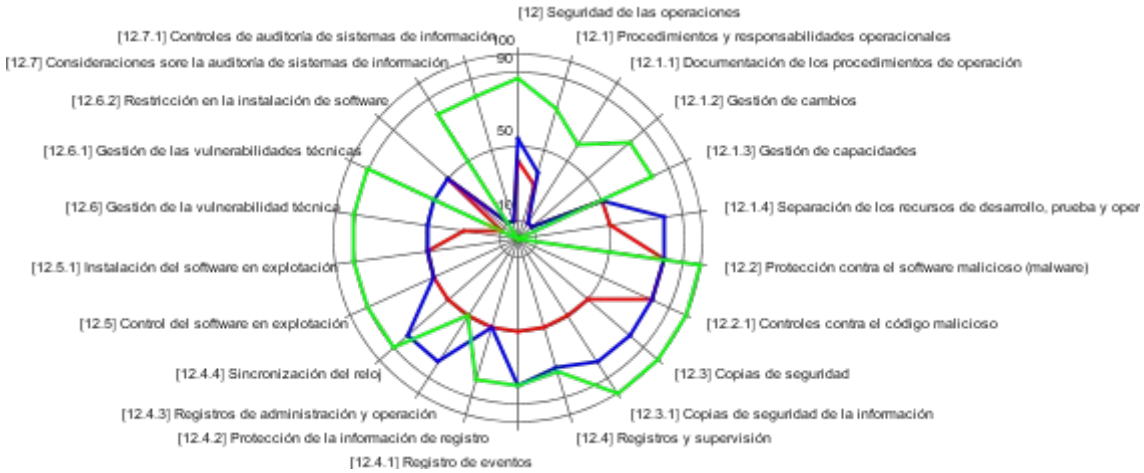

Figura 43 - Auditoría ISO 27002 - Seguridad de las operaciones

6.2.2.9. Seguridad de las comunicaciones

control	Anterior	Actual
[13] Seguridad de las comunicaciones	L1-L3	L1-L3
[13.1] Gestión de la seguridad de redes	L2-L3	L2-L3
[13.1.1] Controles de red	L2	L2
[13.1.2] Seguridad de los servicios de red	L3	L3
[13.1.3] Segregación en redes	L2	L3
[13.2] Intercambio de información	L1-L3	L1-L3
[13.2.1] Políticas y procedimientos de intercambio de información	L2	L2
[13.2.2] Acuerdos de intercambio de información	L3	L3
[13.2.3] Mensajería electrónica	L1	L1
[13.2.4] Acuerdos de confidencialidad o no revelación	L3	L3

Tabla 127: Auditoría ISO 27002 - Seguridad de las comunicaciones

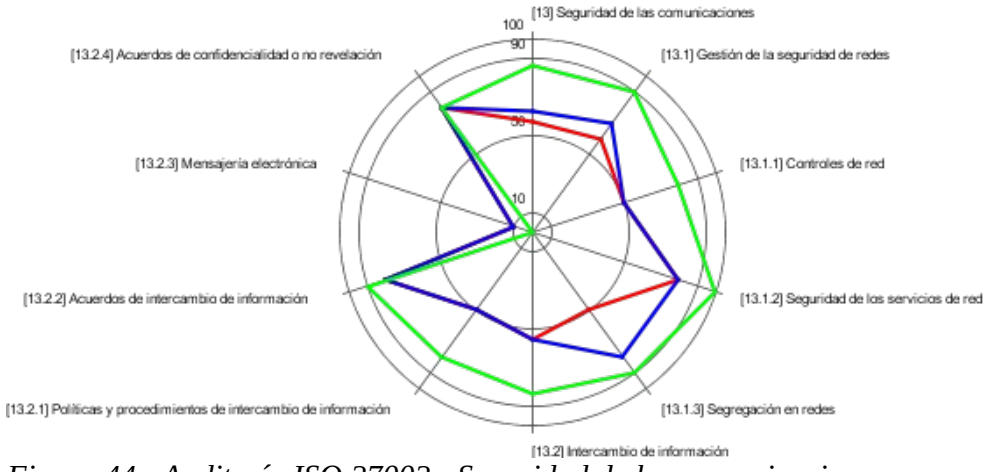

Figura 44 - Auditoría ISO 27002 - Seguridad de las comunicaciones

6.2.2.10. Adquisición, desarrollo y mantenimiento de sistemas de información

control	Anterior	Actual
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información	L1-L3	_-L3
[14.1] Requisitos de seguridad en sistemas de información	L1-L2	L1-L2
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	L2	L2
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas	L2	L2
[14.1.3] Protección de las transacciones de servicios de aplicaciones	L1	L1
[14.2] Seguridad en el desarrollo y en los procesos de soporte	L2-L3	_-L3
[14.2.1] Política de desarrollo seguro	L3	L3
[14.2.2] Procedimiento de control de cambios en sistemas	L3	L3
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L2	L2
[14.2.4] Restricciones a los cambios en los paquetes de software	L2	L2
[14.2.5] Principios de ingeniería de sistemas seguros	L2	L2
[14.2.6] Entorno de desarrollo seguro	n.a.	
[14.2.7] Externalización del desarrollo de software	L3	L3
[14.2.8] Pruebas funcionales de seguridad de sistemas	L2	L3
[14.2.9] Pruebas de aceptación de sistemas	L2	L3
[14.3] Datos de prueba	L2	L3
[14.3.1] Protección de los datos de prueba	L2	L3

Tabla 128: Auditoría ISO 27002 - Adquisición, desarrollo y mantenimiento de sistemas de información

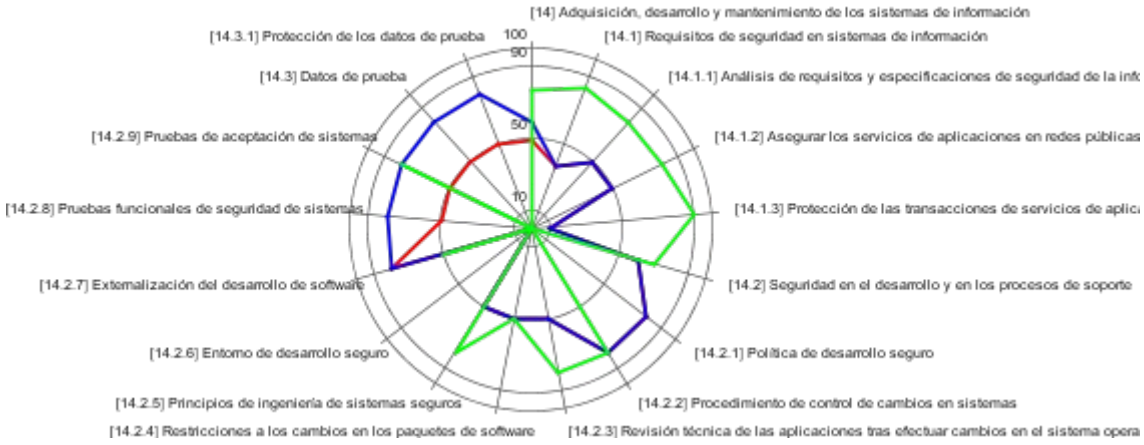

Figura 45 - Auditoría ISO 27002 - Adquisición, desarrollo y mantenimiento de sistemas de información

6.2.2.11. Relación con proveedores

control	Anterior	Actual
[15] Relación con proveedores	L2-L3	L2-L3
[15.1] Seguridad en las relaciones con proveedores	L2-L3	L2-L3
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores	L2	L2
[15.1.2] Requisitos de seguridad en contratos con terceros	L3	L3
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones	L3	L3
[15.2] Gestión de la provisión de servicios del proveedor	L3	L3
[15.2.1] Control y revisión de la provisión de servicios del proveedor	L3	L3
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor	L3	L3

Tabla 129: Auditoría ISO 27002 - Relación con proveedores

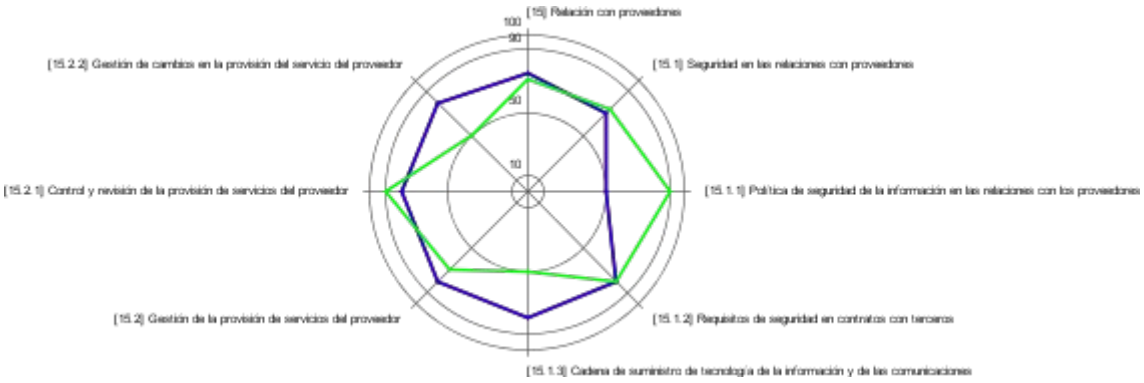

Figura 46 - Auditoría ISO 27002 - Relación con proveedores

6.2.2.12. Gestión de incidentes de seguridad de la información

control	Anterior	Actual
[16] Gestión de incidentes de seguridad de la información	L1-L2	L2-L3
[16.1] Gestión de incidentes de seguridad de la información y mejoras	L1-L2	L2-L3
[16.1.1] Responsabilidades y procedimientos	L1	L2
[16.1.2] Notificación de eventos de seguridad de la información	L1	L2
[16.1.3] Notificación de puntos débiles de la seguridad	L1	L2
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información	L2	L3
[16.1.5] Respuesta a incidentes de seguridad de la información	L2	L3
[16.1.6] Aprendizaje de los incidentes de seguridad de la información	L1	L3

control	Anterior	Actual
[16.1.7] Recopilación de evidencias	L1	L3

Tabla 130: Auditoría ISO 27002 - Gestión de incidentes de seguridad de la información

Figura 47 - Auditoría ISO 27002 - Gestión de incidentes de seguridad de la información

6.2.2.13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

control	Anterior	Actual
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio	L1-L3	L1-L3
[17.1] Continuidad de la seguridad de la información	L1-L2	L1-L2
[17.1.1] Planificación de la continuidad de la seguridad de la información	L2	L2
[17.1.2] Implementar la continuidad de la seguridad de la información	L2	L2
[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L1	L1
[17.2] Redundancia	L3	L3
[17.2.1] Disponibilidad de los recursos de tratamiento de la información	L3	L3

Tabla 131: Auditoría ISO 27002 - Aspectos de seguridad de la información para la gestión de la continuidad del negocio

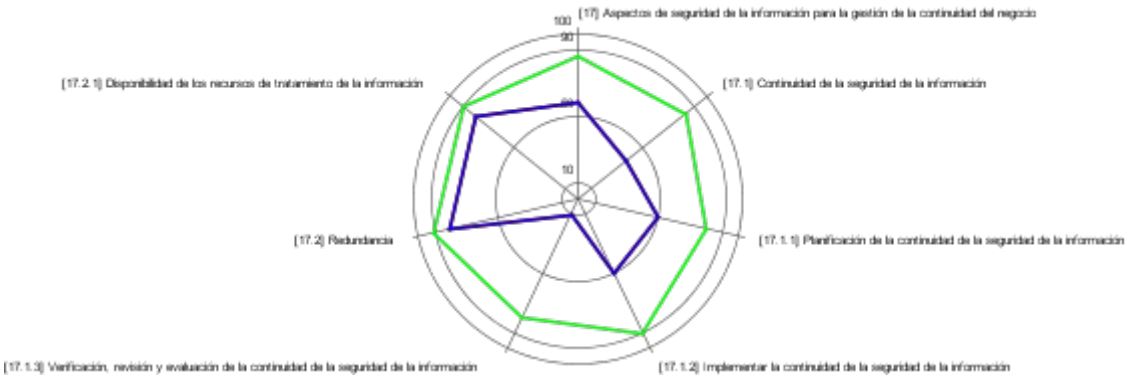

Figura 48 - Auditoría ISO 27002 - Aspectos de seguridad de la información para la gestión de la continuidad del negocio

6.2.2.14. Cumplimiento

control	Anterior	Actual
[18] Cumplimiento	L0-L2	L0-L3
[18.1] Cumplimiento de los requisitos legales y contractuales	L1-L2	L1-L2
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales	L1	L1
[18.1.2] Derechos de propiedad intelectual (DPI)	L2	L2
[18.1.3] Protección de los registros de la organización	L2	L2
[18.1.4] Protección y privacidad de la información de carácter personal	L1	L1
[18.1.5] Regulación de los controles criptográficos	L1	L2
[18.2] Revisiones de la seguridad de la información	L0-L1	L0-L3
[18.2.1] Revisión independiente de la seguridad de la información	L0	L0
[18.2.2] Cumplimiento de las políticas y normas de seguridad	L0	L3
[18.2.3] Comprobación del cumplimiento técnico	L1	L2

Tabla 132: Auditoría ISO 27002 - Cumplimiento

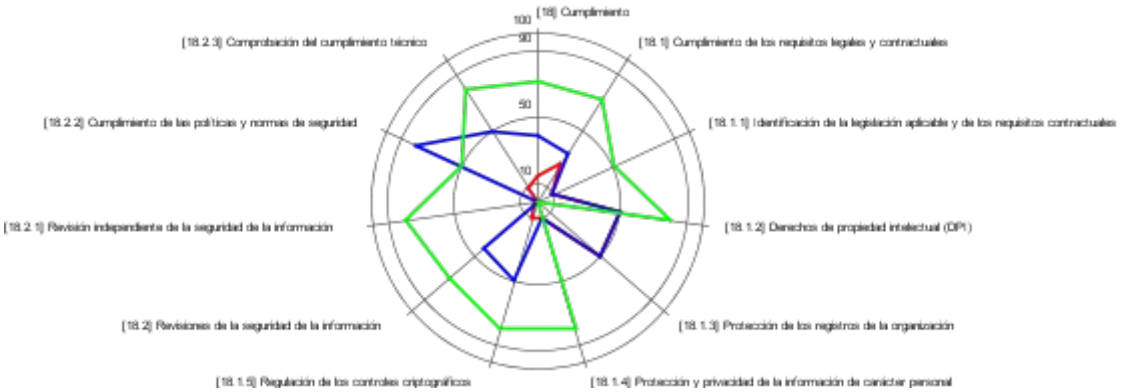

Figura 49 - Auditoría ISO 27002 - Cumplimiento

6.3. Presentación de resultados.

6.3.1. Resultados sintéticos

A continuación presentamos los resultados sintéticos para el Esquema Nacional de seguridad atendiendo a los distintos Marcos, podremos observar en rojo la situación "Anterior", en azul la situación "Actual" y se añade en verde la recomendación de cumplimiento hecha por PILAR:

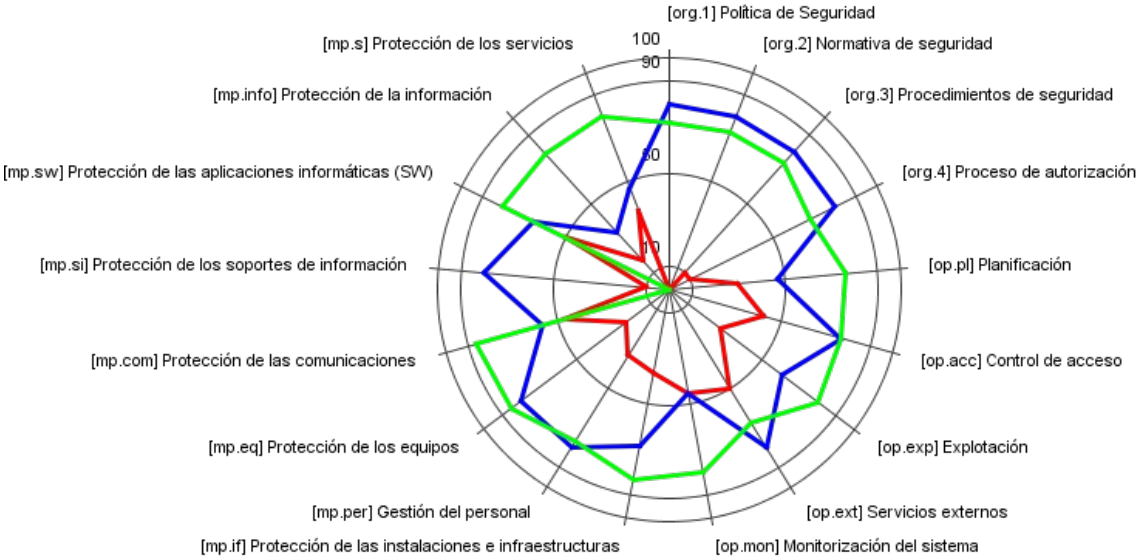

Figura 50 - Auditoría ENS - Resultado sintético por marcos

A continuación presentamos el resultado sintético para ISO/IEC 27002:2013 atendiendo a los distintos dominios, podemos observar en rojo la situación "Anterior", en azul la situación "Actual" y se añade en verde la recomendación de cumplimiento hecha por PILAR:

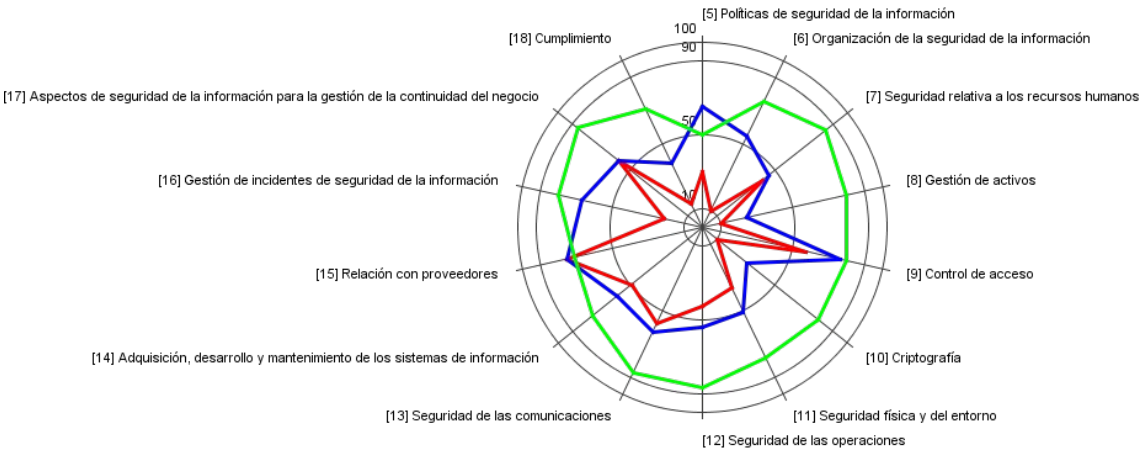

Figura 51 - Auditoría ISO 27002 - Resultado sintético por dominios

6.3.2. Hallazgos

Los hallazgos propuestos no son un listado completo que revise todas las salvaguardas de cada control de los estándares si no que más bien se trataría a modo ejemplo de una auditoría que revise al menos una de las salvaguardas de cada control y acorde a ella establecer el nivel de la disconformidad, en un entorno real sería necesaria una revisión de todas las salvaguardas.

6.3.2.1. Esquema Nacional de Seguridad

ID: ENS-NC-1-01	**Control ENS**: [org.3] Procedimientos de seguridad	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe documentación sobre cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea ó cómo identificar comportamientos anómalos.		
Acción correctiva: Org-01-XX		

Tabla 133: Hallazgos – No Conformidad Mayor - ENS org.3

ID: ENS-NC-1-02	**Control ENS**: [org.4] Proceso de autorización	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe un proceso formal sobre autorizaciones que cubra todos los elementos del sistema de información para: • Utilización de instalaciones, habituales y alternativas. • Entrada de equipos en producción, en particular, equipos que involucren criptografía. • Entrada de aplicaciones en producción. • Establecimiento de enlaces de comunicaciones con otros sistemas. • Utilización de medios de comunicación, habituales y alternativos. • Utilización de soportes de información. • Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga. • Utilización se servicios externos, bajo contrato o convenio.		
Acción correctiva: Org-02-XX		

Tabla 134: Hallazgos – No Conformidad Mayor - ENS org.4

ID: ENS-NC-1-03	**Control ENS**: [op.pl.2] Arquitectura de seguridad	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe un planteamiento integral detallando, al menos, los sistema de gestión relativos a la planificación, organización y control de los recursos de la seguridad de la información para una categoría MEDIA.		
Acción correctiva: Pl-01-XX		

Tabla 135: Hallazgos – No Conformidad Mayor - ENS op.pl.2

ID: ENS-NC-1-04	**Control ENS**: [mp.if.1] Áreas separadas y con control de acceso	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se están controlando los accesos a todas las áreas donde existen sistemas de información de forma que sólo se pueda acceder por las entradas previstas y vigiladas.		
Acción correctiva: If-01-XX		

Tabla 136: Hallazgos – No Conformidad Mayor - ENS mp.if.1

ID: ENS-NC-1-05	**Control ENS**: [mp.info.4] Firma electrónica	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe documentación sobre la política de firma electrónica, ni de los requerimientos que estos mecanismos deban cumplir.		
Acción correctiva: Info-03-XX		

Tabla 137: Hallazgos – No Conformidad Mayor - ENS mp.info.4

ID: ENS-NC-1-06	**Control ENS**: [mp.info.5] Sellos de tiempo	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe documentación sobre los requerimientos que estos mecanismos deban cumplir.		
Acción correctiva: Info-04-XX		

Tabla 138: Hallazgos – No Conformidad Mayor - ENS mp.info.5

ID: ENS-NC-1-07	**Control ENS**: [mp.s.1] Protección del correo electrónico (e-mail)	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: La información distribuida por medio de correo electrónico, no se está protegiendo adecuadamente. No se han establecido normas de uso del correo electrónico por parte del personal.		
Acción correctiva: S-01-XX		

Tabla 139: Hallazgos – No Conformidad Mayor - ENS mp.s.1

ID: ENS-NC-1-08	**Control ENS**: [mp.s.8] Protección frente a la denegación de servicio	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se está protegiendo al Ayuntamiento frente a ataques de “cross site scripting”. No existe documentación sobre las medidas de protección frente a la denegación de servicio implantadas.		
Acción correctiva: S-02-XX		

Tabla 140: Hallazgos – No Conformidad Mayor - ENS mp.s.8

ID: ENS-NC-2-01	**Control ENS**: [op.pl.3] Adquisición de nuevos componentes	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe un proceso formal documentado para planificar la adquisición de nuevos componentes del sistema.		
Acción correctiva: Pl-02-XX		

Tabla 141: Hallazgos – No Conformidad Menor - ENS op.pl.3

ID: ENS-NC-2-02	**Control ENS**: [op.pl.4] Dimensionamiento / Gestión de capacidades	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Con carácter previo a la puesta en explotación, no se está realizando de forma documentada un estudio previo que cubra los siguientes aspectos: • Necesidades de procesamiento. • Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse. • Necesidades de comunicación. • Necesidades de personal: cantidad y cualificación profesional. • Necesidades de instalaciones y medios auxiliares. Si bien se escriben en los pliegos estos no forman parte de un estudio previo.		
Acción correctiva: Pl-03-XX		

Tabla 142: Hallazgos – No Conformidad Menor - ENS op.pl.4

ID: ENS-NC-2-03	**Control ENS**: [op.exp.1] Inventario de activos	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: Se mantiene un inventario actualizado de todos los elementos del sistema, detallando su naturaleza pero no se identifica a su propietario; es decir, a la persona que es responsable de las decisiones relativas al mismo.		
Acción correctiva: Exp-01-XX		

Tabla 143: Hallazgos – No Conformidad Menor - ENS op.exp.1

ID: ENS-NC-2-04	**Control ENS**: [op.exp.4] Mantenimiento	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe documentación sobre las acciones de mantenimiento (físico y lógico). Tampoco se registran estas acciones y sus resultados.		
Acción correctiva: Exp-02-XX		

Tabla 144: Hallazgos – No Conformidad Menor - ENS op.exp.4

ID: ENS-NC-2-05	**Control ENS**: [op.exp.11] Protección de claves criptográficas	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existen documentación ni constancia de que las claves criptográficas se estén protegiendo durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.		
Acción correctiva: Exp-04-XX		

Tabla 145: Hallazgos – No Conformidad Menor - ENS op.exp.11

ID: ENS-NC-2-06	**Control ENS**: [op.mon.2] Sistema de métricas	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se está realizando un procedimiento que establezca los indicadores, métrica asociada y designación de responsables para la recopilación de los elementos necesarios para dar respuesta a la encuesta INES.		
Acción correctiva: Mon-01-XX		

Tabla 146: Hallazgos – No Conformidad Menor - ENS op.mon.2

ID: ENS-NC-2-07	**Control ENS**: [mp.com.3] Protección de la autenticidad y de la integridad	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe documentación que establezca la necesidad de utilizar redes privadas virtuales para garantizar la autenticidad y la integridad de la información antes de su intercambio.		
Acción correctiva: Com-03-XX		

Tabla 147: Hallazgos – No Conformidad Menor - ENS mp.com.3

ID: ENS-NC-2-08	**Control ENS**: [mp.info.1] Datos de carácter personal	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se han desarrollado las acciones de seguridad necesarias para llevar a cabo la implantación de la normativa de protección de datos (RGPD).		
Acción correctiva: Info-01-XX		

Tabla 148: Hallazgos – No Conformidad Menor - ENS mp.info.1

ID: ENS-NC-2-09	**Control ENS**: [mp.info.2] Calificación de la información	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se han redactado los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere.		
Acción correctiva: Info-02-XX		

Tabla 149: Hallazgos – No Conformidad Menor - ENS mp.info.2

ID: ENS-O-01	**Control ENS**: [op.acc.3] Segregación de funciones y tareas	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se ha organizado el sistema de control de acceso de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.		
Acción correctiva: Acc-01-XX		

Tabla 150: Hallazgos – Observación - ENS op.acc.3

ID: ENS-O-02	**Control ENS**: [op.exp.5] Gestión de cambios externalizada	
Tipo: Observación	**MMC Actual:** n.a.	**MMC Objetivo:** L3 (terceros)
Detalle: No se analizan todos los cambios anunciados por el fabricante o proveedor para determinar su conveniencia para ser incorporados.		
Acción correctiva: Exp-03-XX		

Tabla 151: Hallazgos – Observación - ENS op.exp.5

ID: ENS-O-03	**Control ENS**: [mp.if.4] Energía eléctrica	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No existe documentación que muestre que el sistema de energía eléctrica se pruebe regularmente.		
Acción correctiva: If-02-XX		

Tabla 152: Hallazgos – Observación - ENS mp.if.4

ID: ENS-O-04	**Control ENS**: [mp.if.5] Protección frente a incendios	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se dispone de un sistema de evacuación de humos acorde a la normativa industrial, no se realizan regularmente simulacros de incendio.		
Acción correctiva: If-03-XX		

Tabla 153: Hallazgos – Observación - ENS mp.if.5

ID: ENS-O-05	**Control ENS**: [mp.per.2] Deberes y obligaciones	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No existe difusión del procedimiento sancionador en caso de incumplimiento de los deberes y obligaciones del personal del Ayuntamiento.		
Acción correctiva: Per-01-XX		

Tabla 154: Hallazgos – Observación - ENS mp.per.2

ID: ENS-O-06	**Control ENS**: [mp.com.1] Perímetro seguro	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se revisa periódicamente el tráfico autorizado.		
Acción correctiva: Com-01-XX		

Tabla 155: Hallazgos – Observación - ENS mp.com.1

ID: ENS-O-07	**Control ENS**: [mp.si.1] Etiquetado	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Los usuarios no disponen de medios ni formación para interpretar correctamente el significado de las etiquetas.		
Acción correctiva: Si-01-XX		

Tabla 156: Hallazgos – Observación - ENS mp.si.1

ID: ENS-O-08	**Control ENS**: [mp.si.3] Custodia	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se realizan revisiones periódicas de las listas de distribución y destinatarios autorizados.		
Acción correctiva: Si-02-XX		

Tabla 157: Hallazgos – Observación - ENS mp.si.3

ID: ENS-O-09	**Control ENS**: [mp.si.4] Transporte	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se monitorizan los tiempos excesivos entre envío y recepción.		
Acción correctiva: Si-03-XX		

Tabla 158: Hallazgos – Observación - ENS mp.si.4

ID: ENS-O-10	**Control ENS**: [mp.si.5] Borrado y destrucción	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se mantienen un registro de los soportes destruidos.		
Acción correctiva: Si-04-XX		

Tabla 159: Hallazgos – Observación - ENS mp.si.5

ID: ENS-O-11	**Control ENS**: [mp.info.6] Limpieza de documentos	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se eliminan meta-datos en el proceso de limpieza de documentos.		
Acción correctiva: Info-05-XX		

Tabla 160: Hallazgos – Observación - ENS mp.info.6

ID: ENS-PM-01	**Control ENS**: [mp.com.2] Protección de la confidencialidad	
Tipo: Pos. Mejora	**MMC Actual:** n.a.	**MMC Objetivo:** n.a.
Detalle: Realizar un procedimiento que describa la forma en la cual se protege la confidencialidad de la información cuanto esta discurre por redes fuera del propio dominio de seguridad. El Ayuntamiento no está obligado a realizar esta acción para cumplir con el ENS pero sería recomendable su implementación.		
Acción: Com-02-XX		

Tabla 161: Hallazgos – Posibilidad de Mejora - ENS mp.com.2

ID: ENS-PM-02	**Control ENS**: [mp.sw.1] Desarrollo de aplicaciones	
Tipo: Pos. Mejora	**MMC Actual:** n.a.	**MMC Objetivo:** L3 (terceros)
Detalle: En caso de que se encargue a terceros desarrollo de software, solicitar que se utilicen metodologías de desarrollo seguro y que satisfagan los requisitos necesarios para cumplir con el ENS. El Ayuntamiento no está obligado a realizar esta acción para cumplir con el ENS pero sería recomendable su implementación.		
Acción: SW-01-XX		

Tabla 162: Hallazgos – Posibilidad de Mejora - ENS mp.sw.1

6.3.2.2. ISO/IEC 27002:2013

ID: ISO27002-NC-1-01	**Control ISO 27002**: [6.2.1] Política de dispositivos móviles	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Los dispositivos móviles o portátiles no se almacenan en contenedores de seguridad, no se han determinado sus medidas para la protección física del dispositivo, no se han instalado detectores de violación de la protección física, no existen guías de uso para los usuarios, no disponen de mecanismos de reacción urgente a incidentes.		
Acción correctiva: Org-02-XX		

Tabla 163: Hallazgos – No Conformidad Mayor - ISO27002 6.2.1

ID: ISO27002-NC-1-02	**Control ISO 27002**: [7.2.1] Responsabilidades de gestión	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se disponen de normativas de obligado cumplimiento en el desempeño del puesto de trabajo para el tratamiento de datos clasificados.		
Acción correctiva: Per-01-XX		

Tabla 164: Hallazgos – No Conformidad Mayor - ISO27002 7.2.1

ID: ISO27002-NC-1-03	**Control ISO 27002**: [8.2.1] Clasificación de la información	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se dispone de normativa para el tratamiento de información clasificada.		
Acción correctiva: Info-02-XX		

Tabla 165: Hallazgos – No Conformidad Mayor - ISO27002 8.2.1

ID: ISO27002-NC-1-04	**Control ISO 27002**: [10.1.2] Gestión de claves	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe protección de claves para contenedores criptográficos.		
Acción correctiva: Exp-04-XX		

Tabla 166: Hallazgos – No Conformidad Mayor - ISO27002 10.1.2

ID: ISO27002-NC-1-05	**Control ISO 27002**: [11.1.2] Controles físicos de entrada	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Algunos accesos no permanecen cerrados fuera de las horas de trabajo, debido a labores de limpieza o mantenimiento.		
Acción correctiva: If-01-XX		

Tabla 167: Hallazgos – No Conformidad Mayor - ISO27002 11.1.2

ID: ISO27002-NC-1-06	**Control ISO 27002**: [11.1.3] Seguridad de oficinas, despachos y recursos	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: En muchos momentos del día la seguridad de la instalación es responsabilidad de un único guarda que puede llegar a tardar 20 minutos en llegar a la zona crítica del sistema de información.		
Acción correctiva: If-01-XX		

Tabla 168: Hallazgos – No Conformidad Mayor - ISO27002 11.1.3

ID: ISO27002-NC-1-07	**Control ISO 27002**: [11.1.4] Protección contra las amenazas externas y ambientales	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de un sistema de detección de inundación.		
Acción correctiva: -		

Tabla 169: Hallazgos – No Conformidad Mayor - ISO27002 11.1.4

ID: ISO27002-NC-1-08	**Control ISO 27002**: [11.1.5] El trabajo en áreas seguras	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No todos los accesos permanecen cerrados fuera de las horas de trabajo, especialmente cuando acontecen festejos cerca de la Casa Consistorial.		
Acción correctiva: Pl-01-XX, If-01-XX		

Tabla 170: Hallazgos – No Conformidad Mayor - ISO27002 11.1.5

ID: ISO27002-NC-1-09	**Control ISO 27002**: [11.2.6] Seguridad de los equipos fuera de las instalaciones	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Los equipos son susceptibles de quedar desatendidos en lugares públicos.		
Acción correctiva: Org-02-XX		

Tabla 171: Hallazgos – No Conformidad Mayor - ISO27002 11.2.6

ID: ISO27002-NC-1-10	**Control ISO 27002**: [12.5.1] Instalación del software en explotación	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se están limpiando los almacenes temporales de un modo programado.		
Acción correctiva: Org-02-XX		

Tabla 172: Hallazgos – No Conformidad Mayor - ISO27002 12.5.1

ID: ISO27002-NC-1-11	**Control ISO 27002**: [13.2.1] Políticas y procedimientos de intercambio de información	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se prohíbe la conexión de telefonía móvil a ordenadores que manejen datos sensibles.		
Acción correctiva: Org-01-XX, Com-03-XX		

Tabla 173: Hallazgos – No Conformidad Mayor - ISO27002 13.2.1

ID: ISO27002-NC-1-12	**Control ISO 27002**: [13.2.3] Mensajería electrónica	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se ha definido una política de uso aceptable del correo electrónico.		
Acción correctiva: S-01-XX		

Tabla 174: Hallazgos – No Conformidad Mayor - ISO27002 13.2.3

ID: ISO27002-NC-1-13	**Control ISO 27002**: [13.2.4] Acuerdos de confidencialidad o no revelación	
Tipo: NC Mayor	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se incluyen las cláusulas de confidencialidad en los contratos laborales.		
Acción correctiva: Per-01-XX		

Tabla 175: Hallazgos – No Conformidad Mayor - ISO27002 13.2.4

ID: ISO27002-NC-1-14	**Control ISO 27002**: [14.1.3] Protección de las transacciones de servicios de aplicaciones	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se dispone de normativa de firma electrónica.		
Acción correctiva: Info-03-XX		

Tabla 176: Hallazgos – No Conformidad Mayor - ISO27002 14.1.3

ID: ISO27002-NC-1-15	**Control ISO 27002**: [17.1.1] Planificación de la continuidad de la seguridad de la información	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe un plan de continuidad de la seguridad de la información.		
Acción correctiva: ISO-05-XX		

Tabla 177: Hallazgos – No Conformidad Mayor - ISO27002 17.1.1

ID: ISO27002-NC-1-16	**Control ISO 27002**: [17.1.2] Implementar la continuidad de la seguridad de la información	
Tipo: NC Mayor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe un plan de continuidad de la seguridad de la información.		
Acción correctiva: ISO-05-XX		

Tabla 178: Hallazgos – No Conformidad Mayor - ISO27002 17.1.2

ID: ISO27002-NC-1-17	**Control ISO 27002**: [17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	
Tipo: NC Mayor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe un plan de continuidad de la seguridad de la información.		
Acción correctiva: ISO-05-XX		

Tabla 179: Hallazgos – No Conformidad Mayor - ISO27002 17.1.3

ID: ISO27002-NC-1-18	**Control ISO 27002**: [18.2.1] Revisión independiente de la seguridad de la información	
Tipo: NC Mayor	**MMC Actual:** L0	**MMC Objetivo:** L3
Detalle: No existe una revisión independiente de la seguridad de la información.		
Acción correctiva: ISO-03-XX		

Tabla 180: Hallazgos – No Conformidad Mayor - ISO27002 18.2.1

ID: ISO27002-NC-2-01	**Control ISO 27002**: [5.1.2] Revisión de las políticas para la seguridad de la información	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se revisa regularmente el total de las políticas para la seguridad de la información.		
Acción correctiva: Pl-01-XX		

Tabla 181: Hallazgos – No Conformidad Menor - ISO27002 5.1.2

ID: ISO27002-NC-2-02	**Control ISO 27002**: [6.1.2] Separación de tareas	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Todos los procesos críticos no tienen al menos dos personas para llevarse a cabo. Para el ENS se considera una observación (ENS-O-01) mientras que para ISO/IEC 27002:2013 gana en importancia para convertirse en una No Conformidad Menor.		
Acciones correctivas: Org-02-XX, Acc-01-XX		

Tabla 182: Hallazgos – No Conformidad Menor - ISO27002 6.1.2

ID: ISO27002-NC-2-03	**Control ISO 27002**: [6.1.5] Seguridad de la información en la gestión de proyectos	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: Los objetivos de seguridad de la información no se incluyen en los objetivos del proyecto y las implicaciones para la seguridad de la información no se abordan y revisan regularmente en todos los proyectos.		
Acción correctiva: SW-01-XX		

Tabla 183: Hallazgos – No Conformidad Menor - ISO27002 6.1.5

ID: ISO27002-NC-2-04	**Control ISO 27002**: [7.2.2] Concienciación, educación y capacitación en seguridad de la información	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe un procedimiento de reacción y prevención frente a spam, phishing y ataques de ingeniería social.		
Acción correctiva: S-01-XX		

Tabla 184: Hallazgos – No Conformidad Menor - ISO27002 7.2.2

ID: ISO27002-NC-2-05	**Control ISO 27002**: [7.3.1] Responsabilidades ante la finalización o cambio	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: A la finalización de la relación laboral no existe procedimiento de recuperación de los dispositivos asignados.		
Acción correctiva: Per-01-XX		

Tabla 185: Hallazgos – No Conformidad Menor - ISO27002 7.3.1

ID: ISO27002-NC-2-06	**Control ISO 27002**: [8.1.1] Inventario de activos	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se dispone de un inventario software, ni de un registro software de base, ni de un registro de sistemas operativos, tampoco se identifica al responsable. No se dispone de un registro de activos de información.		
Acción correctiva: Pl-01-XX, Exp-01-XX		

Tabla 186: Hallazgos – No Conformidad Menor - ISO27002 8.1.1

ID: ISO27002-NC-2-07	**Control ISO 27002**: [8.1.2] Propiedad de los activos	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se identifica a los propietarios de los activos software ni de los activos de información.		
Acción correctiva: Exp-01-XX, Info-02-XX		

Tabla 187: Hallazgos – No Conformidad Menor - ISO27002 8.1.2

ID: ISO27002-NC-2-08	**Control ISO 27002**: [8.1.4] Devolución de activos	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: A la finalización de la relación laboral no existe procedimiento de recuperación de los dispositivos asignados.		
Acción correctiva: Per-01-XX		

Tabla 188: Hallazgos – No Conformidad Menor - ISO27002 8.1.4

ID: ISO27002-NC-2-09	**Control ISO 27002**: [8.2.3] Manipulado de la información	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: Todos los soportes no se guardan en lugar seguro cuando no están en uso.		
Acción correctiva: Info-02-XX		

Tabla 189: Hallazgos – No Conformidad Menor - ISO27002 8.2.3

ID: ISO27002-NC-2-10	**Control ISO 27002**: [8.3.1] Gestión de soportes extraíbles	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No tienen formación completa los administradores de sistemas en gestión de soportes.		
Acción correctiva: Org-02-XX, Si-01-XX, Si-02-XX		

Tabla 190: Hallazgos – No Conformidad Menor - ISO27002 8.3.1

ID: ISO27002-NC-2-11	**Control ISO 27002**: [8.3.2] Eliminación de soportes	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se dispone de una normativa que determine qué información debe ser eliminada de forma segura.		
Acción correctiva: Si-04-XX		

Tabla 191: Hallazgos – No Conformidad Menor - ISO27002 8.3.2

ID: ISO27002-NC-2-12	**Control ISO 27002**: [8.3.3] Soportes físicos en tránsito	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de normativa para el transporte de soportes.		
Acción correctiva: Si-03-XX		

Tabla 192: Hallazgos – No Conformidad Menor - ISO27002 8.3.3

ID: ISO27002-NC-2-13	**Control ISO 27002**: [10.1.1] Política de uso de los controles criptográficos	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de un normativa sobre firma electrónica.		
Acción correctiva: Com-02-XX, Com-03-XX, Info-03-XX		

Tabla 193: Hallazgos – No Conformidad Menor - ISO27002 10.1.1

ID: ISO27002-NC-2-14	**Control ISO 27002**: [11.2.1] Emplazamiento y protección de equipos	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Los equipos sensibles no se instalan en áreas separadas.		
Acción correctiva: If-01-XX, If-03-XX		

Tabla 194: Hallazgos – No Conformidad Menor - ISO27002 11.2.1

ID: ISO27002-NC-2-15	**Control ISO 27002**: [11.2.2] Instalaciones de suministro	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe alarma en tiempo real para cuando el sistema de climatización sale de especificaciones.		
Acción correctiva: -		

Tabla 195: Hallazgos – No Conformidad Menor - ISO27002 11.2.2

ID: ISO27002-NC-2-16	**Control ISO 27002**: [11.2.5] Retirada de materiales propiedad de la empresa	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: El activo se revisa a su regreso, se revisa antes de la siguiente entrega.		
Acción correctiva: Org-02-XX, Si-03-XX		

Tabla 196: Hallazgos – No Conformidad Menor - ISO27002 11.2.5

ID: ISO27002-NC-2-17	**Control ISO 27002**: [12.1.1] Documentación de los procedimientos de operación	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No existe documentación técnica completa de los componentes del sistema.		
Acción correctiva: Org-01-XX		

Tabla 197: Hallazgos – No Conformidad Menor - ISO27002 12.1.1

ID: ISO27002-NC-2-18	**Control ISO 27002**: [12.1.2] Gestión de cambios	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3

Detalle: No se hace un seguimiento permanente de los servicios externos.
Acción correctiva: Exp-03-XX

Tabla 198: Hallazgos – No Conformidad Menor - ISO27002 12.1.2

ID: ISO27002-NC-2-19	**Control ISO 27002**: [12.1.3] Gestión de capacidades	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se estudia la dependencia con otros servicios a la hora de planificar capacidades.		
Acción correctiva: Pl-03-XX		

Tabla 199: Hallazgos – No Conformidad Menor - ISO27002 12.1.3

ID: ISO27002-NC-2-20	**Control ISO 27002**: [12.4.2] Protección de la información de registro	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se está llevando a cabo la protección de la información de los registros.		
Acción correctiva: ISO-04-XX		

Tabla 200: Hallazgos – No Conformidad Menor - ISO27002 12.4.2

ID: ISO27002-NC-2-21	**Control ISO 27002**: [12.6.1] Gestión de las vulnerabilidades técnicas	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Antes de introducir nuevos elementos en el sistema no se realiza un análisis previo basado en el conocimiento exhaustivo del sistema ni se identifican las vulnerabilidades potenciales a partir del análisis previo		
Acción correctiva: Exp-02-XX		

Tabla 201: Hallazgos – No Conformidad Menor - ISO27002 12.6.1

ID: ISO27002-NC-2-22	**Control ISO 27002**: [12.7.1] Controles de auditoría de sistemas de información	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se han acordado los requerimientos ni se ha documentado el procedimiento.		
Acción correctiva: ISO-01-XX		

Tabla 202: Hallazgos – No Conformidad Menor - ISO27002 12.7.1

ID: ISO27002-NC-2-23	**Control ISO 27002**: [14.1.1] Análisis de requisitos y especificaciones de seguridad de la información	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se identifican los requisitos técnicos de seguridad antes de la adquisición de nuevos componentes.		
Acción correctiva: Pl-02-XX		

Tabla 203: Hallazgos – No Conformidad Menor - ISO27002 14.1.1

ID: ISO27002-NC-2-24	**Control ISO 27002**: [14.1.2] Asegurar los servicios de aplicaciones en redes públicas	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se revisan regularmente las vulnerabilidades de los algoritmos de cifrado.		
Acción correctiva: Com-02-XX, Com-03-XX		

Tabla 204: Hallazgos – No Conformidad Menor - ISO27002 14.1.2

ID: ISO27002-NC-2-25	**Control ISO 27002**: [14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: En equipos externalizados se desconoce si se prueban previamente los cambios en un equipo que no se encuentre en producción.		
Acción correctiva: Exp-03-XX		

Tabla 205: Hallazgos – No Conformidad Menor - ISO27002 14.2.3

ID: ISO27002-NC-2-26	**Control ISO 27002**: [14.2.4] Restricciones a los cambios en los paquetes de software	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: En equipos externalizados se desconoce si se prueban previamente los cambios en un equipo que no se encuentre en producción.		
Acción correctiva: Org-02-XX, Exp-03-XX		

Tabla 206: Hallazgos – No Conformidad Menor - ISO27002 14.2.4

ID: ISO27002-NC-2-27	**Control ISO 27002**: [14.2.5] Principios de ingeniería de sistemas seguros	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro antes de que este se produzca.		
Acción correctiva: Pl-01-XX, SW-01-XX		

Tabla 207: Hallazgos – No Conformidad Menor - ISO27002 14.2.5

ID: ISO27002-NC-2-28	**Control ISO 27002**: [15.1.1] Política de seguridad de la información en las relaciones con los proveedores	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de una normativa de autorización de acceso y concesión de privilegios para usuarios administrados por proveedores.		
Acción correctiva: Org-02-XX		

Tabla 208: Hallazgos – No Conformidad Menor - ISO27002 15.1.1

ID: ISO27002-NC-2-29	**Control ISO 27002**: [16.1.1] Responsabilidades y procedimientos	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: Los planes de continuidad no tienen en cuenta posibles infecciones por código dañino.		
Acción correctiva: Org-01-XX		

Tabla 209: Hallazgos – No Conformidad Menor - ISO27002 16.1.1

ID: ISO27002-NC-2-30	**Control ISO 27002**: [16.1.2] Notificación de eventos de seguridad de la información	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No existe documentación sobre canales oficiales definidos para la comunicación de los incidentes.		
Acción correctiva: Org-01-XX		

Tabla 210: Hallazgos – No Conformidad Menor - ISO27002 16.1.2

ID: ISO27002-NC-2-31	**Control ISO 27002**: [18.1.2] Derechos de propiedad intelectual (DPI)	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de documentos que acrediten la propiedad intelectual.		
Acción correctiva: Org-01-XX		

Tabla 211: Hallazgos – No Conformidad Menor - ISO27002 18.1.2

ID: ISO27002-NC-2-32	**Control ISO 27002**: [18.1.3] Protección de los registros de la organización	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se cumplen los requisitos de continuidad de negocio para los registros de la organización.		
Acción correctiva: ISO-02-XX		

Tabla 212: Hallazgos – No Conformidad Menor - ISO27002 18.1.3

ID: ISO27002-NC-2-33	**Control ISO 27002**: [18.1.4] Protección y privacidad de la información de carácter personal	
Tipo: NC Menor	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: No se han establecido directrices de clasificación para datos de carácter personal. No se han definido responsabilidades sobre datos de carácter personal. No se ha contemplado la protección de la información de carácter personal.		
Acción correctiva: Info-01-XX		

Tabla 213: Hallazgos – No Conformidad Menor - ISO27002 18.1.4

ID: ISO27002-NC-2-34	**Control ISO 27002**: [18.1.5] Regulación de los controles criptográficos	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se tienen en cuenta los requisitos legales y contractuales en algunos de los activos obligados a disponer de controles criptográficos.		
Acción correctiva: Com-02-XX, Info-03-XX		

Tabla 214: Hallazgos – No Conformidad Menor - ISO27002 18.1.5

ID: ISO27002-NC-2-35	**Control ISO 27002**: [18.2.3] Comprobación del cumplimiento técnico	
Tipo: NC Menor	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se dispone de documentación para la revisión del cumplimiento de los requisitos técnicos de los sistemas de información.		
Acción correctiva: Org-01-XX		

Tabla 215: Hallazgos – No Conformidad Menor - ISO27002 18.2.3

ID: ISO27002-O-01	**Control ISO 27002**: [7.1.2] Términos y condiciones del empleo	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No existe compromiso escrito de cumplimiento de la política y la normativa correspondiente.		
Acción correctiva: Per-01-XX		

Tabla 216: Hallazgos – Observación - ISO27002 7.1.2

ID: ISO27002-O-02	**Control ISO 27002**: [7.2.3] Proceso disciplinario	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No existe difusión del procedimiento sancionador en caso de incumplimiento de los deberes y obligaciones del personal del Ayuntamiento.		
Acción correctiva: Per-01-XX		

Tabla 217: Hallazgos – Observación - ISO27002 7.2.3

ID: ISO27002-O-03	**Control ISO 27002**: [8.2.2] Etiquetado de la información	
Tipo: Observación	**MMC Actual:** L1	**MMC Objetivo:** L3
Detalle: Los usuarios no disponen de medios y formación para interpretar correctamente lo significado por las etiquetas.		
Acción correctiva: Si-01-XX, Info-02-XX		

Tabla 218: Hallazgos – Observación - ISO27002 8.2.2

ID: ISO27002-O-04	**Control ISO 27002**: [11.1.1] Perímetro de seguridad física	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Las salidas de emergencia no garantizan que solo el personal autorizado pueda acceder a las instalaciones y una de ellas se utiliza como entrada y salida habitual.		
Acción correctiva: If-01-XX		

Tabla 219: Hallazgos – Observación - ISO27002 11.1.1

ID: ISO27002-O-05	**Control ISO 27002**: [11.2.4] Mantenimiento de los equipos	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se hace un seguimiento permanente de actualizaciones.		
Acción correctiva: Exp-02-XX		

Tabla 220: Hallazgos – Observación - ISO27002 11.2.4

ID: ISO27002-O-06	**Control ISO 27002**: [11.2.7] Reutilización o eliminación segura de equipos	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se dispone de normativa para la retirada de equipamiento (HW) de producción.		
Acción correctiva: Si-04-XX		

Tabla 221: Hallazgos – Observación - ISO27002 11.2.7

ID: ISO27002-O-07	**Control ISO 27002**: [12.1.4] Separación de los recursos de desarrollo, prueba y operación	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Se desconoce si los terceros separan los recursos de desarrollo, pruebas y operación.		
Acción correctiva: SW-01-XX		

Tabla 222: Hallazgos – Observación - ISO27002 12.1.4

ID: ISO27002-O-08	**Control ISO 27002**: [13.1.2] Seguridad de los servicios de red	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se revisan regularmente los usuarios y procesos autorizados.		
Acción correctiva: Org-02-XX, Com-01-XX, Com-02-XX, Com-03-XX		

Tabla 223: Hallazgos – Observación - ISO27002 13.1.2

ID: ISO27002-O-09	**Control ISO 27002**: [14.2.1] Política de desarrollo seguro	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Se desconoce si los terceros disponen de una política de desarrollo seguro.		
Acción correctiva: SW-01-XX		

Tabla 224: Hallazgos – Observación - ISO27002 14.2.1

ID: ISO27002-O-10	**Control ISO 27002**: [14.2.2] Procedimiento de control de cambios en sistemas	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se han designado responsables para abortar y, en su caso recuperar, la situación inicial antes de un cambio.		
Acción correctiva: Exp-03-XX, SW-01-XX		

Tabla 225: Hallazgos – Observación - ISO27002 14.2.2

ID: ISO27002-O-11	**Control ISO 27002**: [14.2.8] Pruebas funcionales de seguridad de sistemas	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Se desconoce si los terceros realizan pruebas funcionales de seguridad de sistemas en entornos pre-producción.		
Acción correctiva: SW-01-XX		

Tabla 226: Hallazgos – Observación - ISO27002 14.2.8

ID: ISO27002-O-12	**Control ISO 27002**: [14.3.1] Protección de los datos de prueba	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: Se desconoce si los terceros protegen los datos de prueba o utilizan datos reales de sus clientes.		
Acción correctiva: SW-01-XX		

Tabla 227: Hallazgos – Observación - ISO27002 14.3.1

ID: ISO27002-O-13	**Control ISO 27002**: [15.2.2] Gestión de cambios en la provisión del servicio del proveedor	
Tipo: Observación	**MMC Actual:** L3	**MMC Objetivo:** L3
Detalle: No se ha establecido un protocolo formal para la gestión de cambios realizados en los sistemas del proveedor.		
Acción correctiva: Exp-03-XX		

Tabla 228: Hallazgos – Observación - ISO27002 15.2.2

ID: ISO27002-O-14	**Control ISO 27002**: [16.1.3] Notificación de puntos débiles de la seguridad	
Tipo: Observación	**MMC Actual:** L2	**MMC Objetivo:** L3
Detalle: No se han definido criterios para interpretar síntomas y mensajes que aparezcan en pantalla.		
Acción correctiva: Org-01-XX		

Tabla 229: Hallazgos – Observación - ISO27002 16.1.3

7. Conclusiones

"Caminamos a hombros de gigantes"

Potentes organizaciones como ISO o el CCN han dedicado gran parte de sus recursos a construir estándares sólidos capaces de proporcionar incontables directrices que mejoren la seguridad de la información en las organizaciones, tal vasta información sin un buen asesoramiento es capaz de echar para atrás hasta al más intrépido de los responsables de sistemas. Es en este punto donde ingenieros de la seguridad de la información entran a formar parte de comités y reciben cargos como el de responsable de seguridad (o CISO) con el claro objetivo de aprovechar las metodologías de los estándares que se alineen mejor con el modelo de negocio de la organización e involucrar a la alta dirección haciéndola partícipe para que los objetivos de seguridad de la información formen parte de los objetivos globales de la organización.

Este TFM trabaja bajo el contexto específico de una administración local "mediana", un lugar donde la organización tiene el suficiente peso como para deber aplicar complejos estándares pero donde el modelo de negocio al carecer de competencia directa puede no estar bien definido y tanto los dirigentes como empleados pueden no contar con la formación o experiencia suficiente. Bajo esta perspectiva la labor del responsable de seguridad se torna más peliaguda y debe ser más metódica que nunca, convencer a la dirección para que defina una estrategia clara de negocio alineada con la SI y sacar a la luz aquellos departamentos con necesidades prioritarias pero que no las manifiesten son tareas adicionales añadidas al catálogo de servicios del RSEG y que deben tratarse durante el desarrollo de un Plan Director de Seguridad que sin el apoyo de la organización está abocado al fracaso, al menos parcialmente.

Además el RSEG no tiene que perder de vista el objetivo final de la organización que consiste en elevar la satisfacción del ciudadano con los servicios municipales y colocarlo en el centro del dato (data commons), para lograr este objetivo un RSEG debe contar con metodologías innovadoras de trabajo que le permitan estar alerta y no dejarse llevar pasando a formar parte de la maquinaria de la administración pública, las guías de aplicación de ISO/ IEC 25012 adaptadas al entorno en el que nos encontremos pueden ser una buena solución.

Una vez puestos en contexto, a la hora de desarrollar un Plan Director de Seguridad trabajar con la guía CCN-STIC 883B, con los toolkits ISO27K o con herramientas como PILAR, nos hará caminar a hombros de gigantes y aprovechar todos esos estándares desarrollados por especialistas que van a permitir preparar a nuestra organización hacia un entorno cada vez más hostil como es el de la seguridad de la información. No se trata tampoco de aplicar toda la metodología como si de un checklist se tratase y ahí nuevamente entra en juego la capacidad del RSEG a la hora de catalogar y priorizar proyectos atendiendo a sus riesgos, que pueden ser cambiantes,

especialmente en épocas de pandemia como la que vivimos y que pone a prueba más que nunca su capacidad de adaptación y priorización.

Añadir que aunque ISO/IEC 27001:2013 y el ENS son los caminos a seguir, y ambos tienen que ser implantados teniendo en cuenta uno al otro, no es recomendable intentar abordar la certificación de los dos estándares a la vez, sería una labor titánica en un sector donde es mejor dar respuesta inmediata a riesgos elevados antes de que se materialicen sus amenazas causando un grave impacto a la organización que buscar ahorrar costes optimizando los procesos para poder certificarnos a la vez en ambos estándares, por ejemplo, podríamos perder excesivo tiempo elaborando la documentación inicial de ambos estándares, es mejor elaborar la de uno y avanzar al análisis de riesgos. Con esto no queremos decir que no haya que mirar en ningún momento al otro estándar, hay que mirarlo pero sólo lo imprescindible, ¿qué establecemos como imprescindible? Ahí radica la habilidad de un buen RSEG a la hora de adaptarse y priorizar, analicémoslo un segundo:

- En primer lugar establecemos que para una administración pública la prioridad es el ENS frente a ISO/IEC 27001:2013 y así lo marcan las leyes 39/2015 y 40/2015. Por lo que empezaremos con el ENS para posteriormente acercarnos a ISO/ IEC 27001:2013.
- En segundo lugar definiremos toda la documentación necesaria para el ENS agregando, donde se recomiende, menciones a ISO/ IEC 27001:2013 y anotando si parte de la documentación que hemos elaborado tiene correlación con la documentación de ISO/ IEC 27001:2013 o si a pesar de tener el mismo nombre será necesario elaborarla de nuevo bajo los objetivos de ISO, p.e. la declaración de aplicabilidad, aunque nos ayude realizar una conversión de la misma para visualizar mejor las diferencias esta no es correcta para ISO/ IEC 27001:2013.
- En tercer lugar realizamos el análisis de riesgos, es importante seleccionar una metodología adecuada a ambos estándares y aquí MAGERIT se vuelve pieza clave para conseguirlo, este es un paso claro y sencillo hacia el ahorro de costes que no impacta en el tiempo de respuesta ante amenazas.
- En cuarto lugar al decidir las propuestas de mejora es cuando suceden las principales diferencias, aunque ambos estándares coincidirán en muchos de los proyectos prioritarios habrá otros en los que no y aquí es donde tenemos que dar prioridad al ENS frente a ISO/ IEC 27001:2013. Por otro lado ISO/ IEC 25012 nos permitirá establecer una metodología para descartar aquellos proyectos en los que no vale la pena invertir esfuerzo reduciendo su riesgo cuando es mejor partir de cero con un producto nuevo que lo sustituya.
- En quinto lugar al realizar la auditoría de cumplimiento después de aplicar las mejoras observaremos como existen muchas mas no conformidades para ISO/ IEC 27001:2013 que para el ENS, esto es natural porque como ya hemos comentado nuestra prioridad ha sido el ENS.

El ENS es un estándar lo suficientemente maduro como para sugerirnos no solo los proyectos prioritarios si no también los que tenemos que llevar a cabo en el futuro una vez abordados los otros. Estos proyectos de futuro no se deben tratar como un “must do” obligatorio si no más bien como una metodología de consolidación y comprobación de resultados que nos permita decidir después de la auditoría de cumplimiento qué proyectos deben ser los prioritarios en el siguiente ciclo. Adicionalmente en este TFM hemos intentado agregar algunos proyectos futuros ISO que complementasen a los ENS observando para ello los controles ISO que no habían

sido considerados en los proyectos futuros ENS, pero como podemos observar en los hallazgos ISO27002-NC-1-07 y ISO27002-NC-2-15 no lo hemos conseguido al 100% por lo que aunque puede ser en cierto modo útil no lo consideramos óptimo para establecer prioridades futuras, es necesario priorizar ISO/ IEC 27001:2013 para poder desarrollar este punto correctamente.

7.1. Objetivos logrados

- Se ha mejorado la seguridad del sistema integral de información de una administración pública local, al menos en lo relativo a los proyectos prioritarios, es necesario seguir completando un ciclo tras otro hasta dar cumplimiento a los estándares.
- Se ha avanzado en el objetivo de dar cumplimiento al ENS y, aunque no se ha conseguido completamente, sí que podemos decir que se están dando los pasos correctos en su consecución. En cuanto al cumplimiento del ENI al estar este reflejado dentro del ENS también hemos avanzado en este sentido, además se ha incluido un refuerzo al ENS mediante la aplicación de ISO/ IEC 25012 gracias a la inclusión del criterio de “conformidad”.
- Se han implementado buenas prácticas en los SGSI acordes a ISO/ IEC 27001 e ISO/ IEC 27002, podemos constatarlo si observamos la Figura 51 aunque es patente que el haber priorizado el ENS ha hecho que avancemos de un modo más lento en la consecución de este estándar.
- Hemos conseguido establecer nexos de unión entre seguridad y calidad del dato, aunque de un modo muy superficial, tal y como era objetivo de este TFM, se podrían haber tenido en cuenta muchas otras características del dato y haber definido de un modo más granular su valoración. Tampoco se han tenido en cuenta características inherentes a la calidad del dato, aplicar esta metodología hubiese permitido analizar la calidad de los datos obtenidos en nuestros análisis y verificar si nuestra visión de seguridad de la información es lo suficientemente acertada o si por el contrario sería necesario obtener “mejor” información en determinados contextos (sería necesario un entorno real para realizar este estudio).
- Hemos conseguido acercar el gobierno del dato al ciudadano gracias al proyecto C-01-2020, migrar un entorno tan relevante como el económico a un espacio como es el “cloud”, al que en primera instancia podemos ser reacios por temas de seguridad de la información, es un primer paso para poner el data commons a disposición del ciudadano. No desmerecemos el proyecto C-02-2020 que si bien no acerca al ciudadano al gobierno del dato, sí que lo hace con la plantilla municipal, tan importante es acercar este tipo de gobierno al ciudadano como al funcionario que le atiende.
- Sin duda alguna NO hemos conseguido convertir este TFM en una guía práctica de cumplimiento para la Administración Local, ver punto 7.3. para más información.

7.2. Seguimiento de la planificación y la metodologías

El seguimiento de la planificación y las metodologías han sido las adecuadas, si bien es cierto que los apartados de la calidad del dato se han acabado terminando prácticamente en la siguiente fase a la que estaba previsto. Este hecho ha sido debido mayormente a imprevistos en el día a día, aunque finalmente se ha conseguido remontar y hemos podido añadir este aspecto al TFM, aunque haya sido de un modo ligero.

Por otro lado inicialmente se utilizó para trabajar la versión de PILAR con el perfil ISO/ IEC 27001:2013 que no incluye el perfil de seguridad de ENS, no obstante no supuso mayor problema dado que es sencillo migrar los datos a la versión de PILAR con el perfil ENS. Se optó por realizar un “fork” y trabajar en las distintas evaluaciones de madurez empleado en PILAR ficheros distintos, uno para ISO/ IEC 27001:2013 y otro para ENS, esto es debido a que la declaración de aplicabilidad (el documento que debe guiar a la auditoría de certificación) es distinta para cada estándar, bajo mi punto de vista al no perseguir los mismos objetivos ambos estándares no pueden disponer de la misma declaración de aplicabilidad (si bien se parecerá bastante), por ello es mejor trabajar con versiones separadas de PILAR a la hora de tratar con los perfiles de seguridad antes que intentar encajar todo. Sí que es cierto que PILAR reflejará las equivalencias en la versión con el perfil ENS, esos datos nos valdrán para realizar comprobaciones de exactitud. Utilizar ambas versiones de PILAR nos ha permitido además obtener informes y análisis más detallados de ambos estándares por separado.

7.3. Líneas de trabajo futuro

Como hemos comentado en el apartado 7.1. lejos de conseguir convertir este TFM en una guía práctica de cumplimiento para la Administración Local nos hemos quedado a mitad de camino y, si bien es cierto que nos puede valer de esqueleto o de guía de inicio, faltarían una serie de trabajos futuros que nos permitiesen completarla:

1. Es necesario trabajar en averiguar cómo deben de ser los siguientes ciclos en la consecución del ENS y de ISO/ IEC 27001:2013. Al tratarse de una Administración Pública hemos empezado por ENS pero el segundo ciclo tal vez no deba de plantearse desde esta perspectiva, es probable que al realizar un segundo ciclo priorizando ISO/ IEC 27001:2013 acabemos minimizando un mayor número de riesgos que si continuásemos desarrollando el ENS, este segundo ciclo se podría realizar añadiendo las directrices de ISO/IEC 27701. La Administración Pública no pierde clientes por no certificarse en ISO/ IEC 27001:2013 y tampoco es sancionada por no cumplir el ENS, por lo que su objetivo último no es conseguir la certificación es mejorar la Seguridad de la Información.
2. No se ha indagado lo suficiente en protección de los sistemas de información en los entornos móviles y de teletrabajo, en época de pandemia se deben priorizar estas actuaciones, requiere de un estudio más en detalle.
3. Se deben acabar de desarrollar modelos tipo para toda la documentación necesaria, al menos la expuesta en el apartado 3.11.

4. Si bien el estudio de la adecuación al ENI, al RGPD y a la LOPDGDD se encuentra latente en toda la metodología, no se ha dedicado tiempo a volver a realizar un análisis de madurez de estos estándares, sería interesante estudiar si alguna de las acciones tomadas ha perjudicado o dificultado de algún modo su consecución.
5. De ISO/IEC 25012 se ha realizado un estudio superficial, mediante el empleo de herramientas avanzadas como las desarrolladas por Verdugo J, Rodríguez M. [5] es posible que se consiga obtener resultados más concluyentes a la hora de utilizar la calidad del dato en entornos de Administración Pública Local. Además en caso de utilizar características inherentes al dato como pueden ser exactitud, completitud, consistencia, credibilidad, actualidad, etc. podríamos analizar los propios datos recabados con el Análisis de Riesgos (sería necesario aplicar sobre un entorno real el estudio).
6. Es necesario un estudio que consiga unificar la elaboración de un Plan Director de Seguridad con la elaboración del Plan Estratégico de Sistemas de Información y con el Plan de Actuación Municipal. Un éxito colaborativo entre estos tres planes ayudaría a maximizar los éxitos individuales de cada plan, evitaría que un plan no acabase restando a otro, mejoraría los modelos de calificación y priorización de proyectos y en general ayudaría con la gobernanza SITIC.

8. Glosario

10G: 10 Gigabit Ethernet
AA.PP.: Administraciones Públicas
ADL: Agente de Desarrollo Local
ADSL: Asymmetric Digital Subscriber Line
AGE: Administración General del Estado
Análisis GAP: análisis de deficiencias
ANS: Acuerdo de Nivel de Servicio
AR: Análisis de Riesgos
ARO: Annual Rate of Ocurrence
BAS: Breach and Attack Simulation
BD: Base de Datos
BYOD: Bring Your Own Device
CCN: Centro Criptológico Nacional
CD: Calidad del Dato
CERT: Computer Emergency Response Team
CMM: Capability Maturity Model
CPD: Centro de Proceso de Datos
CSI: Comité de Seguridad de la Información
CSIRT: Computer Security Incident Response Team
DdoS: Distributed denial-of-service attack
DHCP: Dynamic Host Configuration Protocol
DIR3: Directorio Común de Unidades Orgánicas y Oficinas
DNS: Domain Name System
DPD: Delegado de Protección de Datos
DQ: Data Quality
EDR: Endpoint Defense and Response
ENI: Esquema Nacional de Interoperabilidad
ENS: Esquema Nacional de Seguridad
ESXi: hipervisor de Vmware
FACE: punto general de entrada de facturas electrónicas de la Administración General del Estado
Firewall UTM: Unified Threat Management Firewall
FNMT: Fábrica Nacional de Moneda y Timbre
FP: Formación Profesional
GIS: Geographic Information System
GLPI: Gestionnaire Libre de Parc Informatique
GPO: Microsoft Group Policy Object
HA: High Availability
IaaS: Infrastructure as a Service
IAM: Informática del Ayuntamiento de Madrid
IDS: Intrusion Detection System
IEC: International Electrotechnical Commission
INSIDE: Infraestructura y Sistemas de Documentación Electrónica del estado.

IOT: Internet Of Things
ISO: International Organization for Standardization
ISP: Internet Service Provider
KMS: Key Managment Server
LAN: Local Area Network
LAPS: Local Administrator Password Solution
LOPD: antigua Ley Orgánica 15/1999 de protección de datos
LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MIT: Massachusetts Institute of Technology
NTI: Norma Técnica de Interoperabilidad
ORVE: Oficina de Registro Virtual
PCE: Plataforma de Contratación del Estado
PDCA: Plan, Do, Check, Act. Ciclo Deming
PPT: Pliego de Prescripciones Técnicas
RAT: Registro de Actividades de Tratamiento del RGPD
RD: Real Decreto
Red SARA: Sistema de Aplicaciones y Redes para las Administraciones
RFID: Radio-frequency identification
RGPD: Reglamento (UE) 2016/679 general de protección de datos
ROR: Responsable de Operaciones de Registro
RRHH: Recursos Humanos
RSEG: Responsable de Seguridad
RSIS: Responsable del Sistema
SaaS: Software as a Service
SAI: Sistema de Alimentación Ininterrumpida
SGSI: Sistema de Gestión de Seguridad de la Información
SGSIENS: SGSI que facilita soporte al ENS
SIA: Sistema de Información Administrativa
SIR: Sistema de Interconexión de Registros
SLA: Service-level agreement
SSGG: Servicios Generales
SSID: Service Set IDentifier
SW: Switch, Software
TFM: Trabajo de Final de Máster
TIC: Tecnologías de la Información y la Comunicación
TWINAX: Twinaxial cabling
UOC: Universitat Oberta de Catalunya
UPS: Uninterruptible Power Supply
VDI: Virtual Desktop Infrastructure
VDP Backup: vSphere Data Protection
VLAN: virtual LAN
VNC: Virtual Network Computing
VPN: Virtual Private Network
vSAN: Virtual Storage Area Network
WAN: Wide Area Network
WSUS: Windows Server Update Services
XML: Extensible Markup Language

9. Bibliografía

[1] Real Decreto 951/2015: https://www.boe.es/eli/es/rd/2015/10/23/951 (Visitado en Septiembre 2020)

[2] CCN-CERT Esquema Nacional de Seguridad – Preguntas frecuentes: https://www.ccn-cert.cni.es/publico/dmpublidocuments/ENS-FAQ.pdf (Visitado en Septiembre 2020)

[3] Real Decreto 4/2010: https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf (Visitado en Septiembre 2020)

[4] Esquema Nacional de Interoperabilidad https://administracionelectronica.gob.es/ctt/eni/descargas (Visitado en Septiembre 2020)

[5] Verdugo J, Rodríguez M. Assessing data cybersecurity using ISO/IEC 25012. Software Quality Journal [Internet]. 2020 [cited 2020 Oct 1];28(3):965. Available from: http://search.ebscohost.com.biblioteca-uoc.idm.oclc.org/login.aspx?direct=true&db=edssjs&AN=edssjs.D4945AB7&site=eds-live&scope=site

[6] Herramienta CLARA del CCN-CERT: https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html (Visitado en Septiembre 2020)

[7] Wiki asignatura SGSI: http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/An%C3%A1lisis+diferencial#Attachments (Visitado en Septiembre 2020)

[8] A16 Gestión de Incidentes de la seguridad de la información: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/ (Visitado en Septiembre 2020)

[9] INSIDE: https://administracionelectronica.gob.es/ctt/inside#.X3dIWOdS9EY (Visitado en Septiembre 2020)

[10] La mala gestión de la calidad del dato aumenta los gastos de las compañías (25 de Febrero de 2015): https://www.computerworld.es/tendencias/la-mala-gestion-de-la-calidad-del-dato-aumenta-los-gastos-de-las-companias (Visitado en Octubre 2020)

[11] Reglamento UE 2016/679 RGPD: https://www.boe.es/doue/2016/119/L00001-00088.pdf (Visitado en Octubre 2020)

[12] Colección de artículos sobre el RGPD: https://rgpd.es/ (Visitado en Octubre 2020)

[13] El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito: https://www.ccn-

cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5476-el-esquema-nacional-de-seguridad-recoge-las-medidas-que-debe-aplicar-el-sector-publico-para-cumplir-con-los-requisitos-del-rgpd-en-este-ambito.html (Visitado en Octubre 2020)

[14] Ley Orgánica 3/2018: https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf (Visitado en Octubre de 2020)

[15] XII Jornadas STIC CCN-CERT (Dr. Carlos Galán): https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3434-m32-02-rgpd-y-ens/file.html (Visitado en Octubre de 2020)

[16] ISO/IEC 27701:2019(en): https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en (Visitado en Octubre de 2020)

[17] ISO 27k toolkit: https://www.iso27001security.com/html/toolkit.html (Visitado en Octubre de 2020)

[18] Guía de Seguridad de las TIC CCN-STIC 883: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3758-ccn-stic-883-guia-de-implantacion-del-ens-para-entidades-locales/file.html (Visitado en Octubre de 2020)

[19] Política de Seguridad de la Información (Red.es): https://www.red.es/redes/sites/redes/files/Poli%CC%81tica%20de%20Seguridad.pdf (Visitado en Octubre de 2020)

[20] ISO27001 Anexo 5.1.1: Política de Seguridad (Andoni Martín): https://urtanta.com/iso27001-anexo-5-1-1-politica-de-seguridad/ (Visitado en Octubre de 2020)

[21] Guía de Seguridad de las TIC CCN-STIC 802: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html (Visitado en Octubre de 2020)

[22] Fase 8 Auditoría Interna según ISO 27001: https://normaiso27001.es/fase-8-auditoria-interna-segun-iso-27001/ (Visitado en Octubre de 2020)

[23] Cuando realizar consultas preliminares al Mercado (Observatorio de Contratación Pública, 26 de Noviembre de 2018): http://www.obcp.es/opiniones/cuando-realizar-las-consultas-preliminares-al-mercado (Visitado en Octubre de 2020)

[24] Guía de Seguridad de las TIC CCN-STIC 815: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html (Visitado en Octubre de 2020)

[25] FASE 9 Revisión por la dirección según ISO 27001: https://normaiso27001.es/fase-9-revision-por-la-direccion-segun-iso-27001/ (Visitado en Octubre de 2020)

[26] Quien debe asistir a la revisión por la Dirección (Club Responsables de Gestión de la Calidad, 2 de Abril de 2013): https://clubresponsablesdecalidad.com/quien-debe-asistir-a-la-revision-por-la-direccion/ (Visitado en Octubre de 2020)

[27] MAGERIT v.3: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (Visitado en Octubre de 2020)

[28] ENS Anexo II Medidas de Seguridad: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1071 (Visitado en Octubre de 2020)

[29] ISO/IEC 25012: https://iso25000.com/index.php/normas-iso-25000/iso-25012 (Visitado en Noviembre de 2020)

[30] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html (Visitado en Noviembre de 2020)

[31] Guía de Seguridad de las TIC CCN-STIC 801: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3803-ccn-stic-882-guia-de-analisis-de-riesgos-para-entidades-locales/file.html (Visitado en Noviembre de 2020)

[32] Guía de Seguridad de las TIC CCN-STIC 852: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4943-ccn-stic-852-aplicacion-del-ens-en-organismos-pagadores/file.html (Visitado en Noviembre de 2020)

[33] Herramienta PILAR del CCN-CERT: https://pilar.ccn-cert.cni.es/ (Visitado en Noviembre de 2020)

[34] Guía para evaluar calidad de datos basada en ISO/IEC 25012 por: Calabrese, Julieta | Esponda, Silvia | Pasini, Ariel C. | Boracchia, Marcos | Pesado, Patricia Mabel. Evento: Congreso Argentino de Ciencias de la Computación (CACIC) (Universidad Nacional de Río Cuarto, Córdoba, 14 al 18 de octubre de 2019) http://sedici.unlp.edu.ar/handle/10915/91086 (Visitado en Noviembre de 2020)

[35] Guía de Seguridad de las TIC CCN-STIC 803: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html (Visitado en Noviembre de 2020)

[36] Guía de Seguridad de las TIC CCN-STIC 804: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_implantacion_del_ens.pdf (Visitado en Noviembre de 2020)

[37] Guía de Seguridad de las TIC CCN-STIC 805: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html (Visitado en Noviembre de 2020)

[38] Guía de Seguridad de las TIC CCN-STIC 806: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf (Visitado en Noviembre de 2020)

[39] Guía de Seguridad de las TIC CCN-STIC 808: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html (Visitado en Noviembre de 2020)

[40] XII Jornadas STIC CCN-CERT (Miguel A. Lubian): https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3377-m31-04-al-final-del-camino-esta-la-recompensa/file.html (Visitado en Noviembre de 2020)

[41] Plataforma de contratación del estado: https://contrataciondelestado.es/ (Visitado en Noviembre de 2020)

[42] PILAR report templates help: http://www.pilar-tools.com/doc/ReportTemplates_74_en_e.pdf (Visitado en Diciembre de 2020)

[43] Real Decreto 3/2010: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330 (Visitado en Diciembre 2020)

[44] Ley 39/2015: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565 (Visitado en Diciembre 2020)

[45] Ley 40/2015: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566 (Visitado en Diciembre 2020)

Diagrama de red y organigrama: Software “DIA” (GNU General Public License, the GPLv2.) http://dia-installer.de/ (Visitado en Septiembre de 2020)

Diagramas de GANTT: Software “GanttProject” (GNU General Public License, the GPLv3.) https://www.ganttproject.biz/ (Visitado en Septiembre de 2020)

10. Anexos

ANEXO I. Organigrama

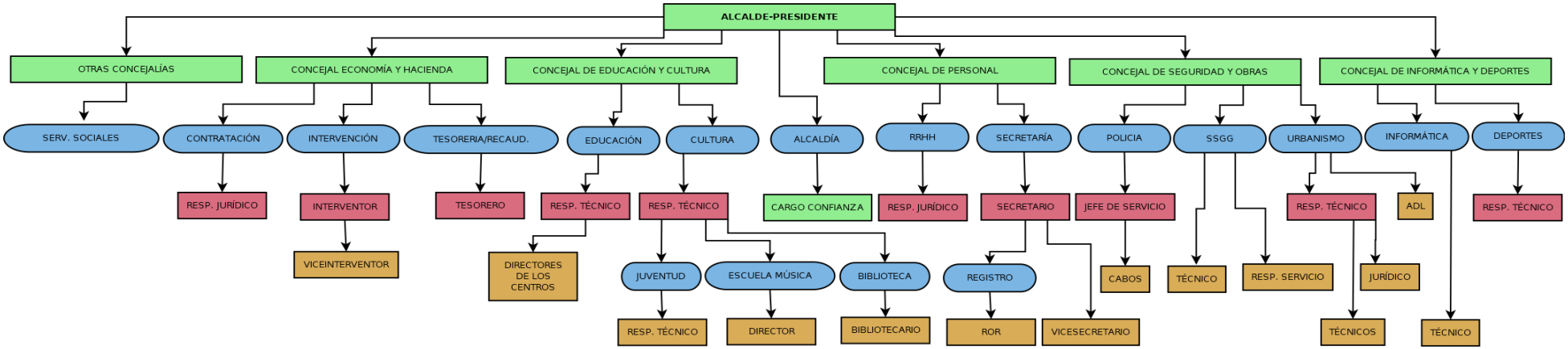

Figura 52 - Organigrama

El organigrama puede no ser exacto.
Los colores indican: Verde, cargos políticos; Azul, departamentos; Rojo, técnicos superiores; Naranja, técnicos medios.
El apartado “otras concejalías” engloba aquellas con escaso personal.

ANEXO II. Diagrama de Estructura Física

Información no disponible

Figura 53 - Diagrama de Infraestructura

ANEXO III. Análisis Diferencial ENI

Se establecen los siguientes niveles: 0% Sin cumplimiento, 25% Cumplimiento Mínimo, 50% Cumplimiento Parcial, 75% Cumplimiento Amplio y 100% Cumplimiento total.

Interoperabilidad organizativa: Cumplimiento Medio.

ART. 8 – Servicios de las Administraciones públicas disponibles por medios electrónicos.

- Establecer y publicar las condiciones para el consumo de los servicios puestos a disposición del resto de entidades por medios electrónicos. (50%)
- Ofrecer los servicios electrónicos a través de la Red SARA u otra red equivalente o conectada a la misma. (50%)
- Realizar el intercambio intermediado de datos a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas conforme a la NTI: (50%)
  - Agentes y roles.
  - Cumplimiento de los requisitos de la Plataforma.
  - Trazabilidad.
  - Catálogo de servicios.

Total cumplimiento: 50% (Cumplimiento del Gestor de Expedientes)

ART. 9 – Inventarios de información administrativa.

- Mantener el Inventario de Información Administrativa (procedimientos y servicios) (SIA). (100%)
- Relación Actualizada de los órganos administrativos, unidades de registro y sus relaciones (DIR3). (50%, Integrados pero con los datos algo desactualizados)

Total cumplimiento: 75%

Interoperabilidad semántica: Cumplimiento Medio

ART. 10 – Activos Semánticos.

- Identificar y publicar los modelos de datos relativos a materiales sujetas a intercambio de información con otras entidades. (50%)
- Emplear definiciones y codificaciones de interés estadístico conformes a la Ley 12/1989, de 9 de mayo de la Función Estadística Pública. (50%)

Total cumplimiento: 50% (Cumplimiento del Gestor de Expedientes).

Interoperabilidad técnica: Cumplimiento Medio-Alto

ART. 11 – Estándares aplicables

- Usar estándares abiertos y, de forma complementaria, estándares de uso generalizado aplicando lo previsto en la NTI de Catálogo de estándares con respecto a:
  - Documentos y expedientes electrónicos puestos a disposición del ciudadano.
  - Aplicaciones y servicios de administración electrónica en sus relaciones con el cuidadano y otras entidades.

Total cumplimiento: 75% (Cumplimiento del Gestor de Expedientes, no es del 100% porque recaudación y contabilidad quedan fuera, se mueven sus datos al gestor de expedientes manualmente)

Infraestructuras y servicios comunes: Cumplimiento Alto

ART. 12 – Uso de infraestructuras y servicios comunes y herramientas genéricas.

- Enlazar las infraestructuras y servicios de la entidad a los correspondientes proporcionados por la AGE. 100%
- Intercambiar asientos registrales a través de ORVE / SIR según lo dispuesto en la NTI de Modelo de datos para el intercambio de asientos entre las entidades registrales. 75%, (No es 100% porque está pendiente la integración del Gestor de Expedientes con SIR)

Comunicaciones de las Administraciones Públicas: Cumplimiento Alto

ART. 13 – Red de comunicaciones de las AA.PP. Españolas
- Conectar la red de la entidad a la Red SARA, cumpliendo lo establecido a tal efecto en la NTI de Requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas. 100%

ART. 14 – Plan de direccionamiento de la Administración.
- Aplicar el Plan de Direccionamiento de la Administración. 100%

ART. 15 – Hora Oficial.
- Sincronizar las aplicaciones y servicios de administración electrónica con la hora oficial a través del Real Instituto y Observatorio de la Armada o utilizar los servicios de la Red SARA que distribuye la hora oficial. 100%

Reutilización y transferencia de tecnología: NO APLICA

ART. 16 – Condiciones de licenciamiento aplicables.
ART. 17 – Directorios de aplicaciones reutilizables.
(El Ayuntamiento no desarrolla software)

Firma electrónica y certificados: Cumplimiento alto

ART. 18 – Interoperabilidad en la política de firma electrónica y de certificados.
- Aprobar y publicar la Política de firma electrónica y de certificados de la entidad:
  - Adoptando la política Marco Firma Electrónica y de certificados de la AGE mediante el mecanismo interno correspondiente.
  - Elaborando una política particular conforme a la NTI de Política de Firma Electrónica y de certificados de la Administración, pudiendo tomar como referencia la Política Marco. (50%, Cumple Gestor de Expedientes, existe ordenanza local de uso de certificado de sede y órgano y hay convenio con entidad certificadora, aunque caducado hay que renovarlo)
- Utilizar los certificados electrónicos definidos en el Capítulo II de la Ley 11/2007 y conformes a la Ley 59/2003 de firma electrónica y sus desarrollos normativos. (100%)
- Garantizar la identificación y autenticación de los ciudadanos en la sede, registro electrónico y resto de servicios electrónicos en la entidad siguiendo lo previsto en el artículo 13 de la Ley 11/2007. (75%, aplicaciones de contabilidad y recaudación no lo permiten)
- Permitir la validación de las firmas electrónicas de los documentos electrónicos recibidos contra la política de firma aprobado. (100%)

Total cumplimiento: 81,25%

ART. 19 – Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación
- Utilizar certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación confiables, es decir, incluidos en la Lista de servicios de confianza publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo. 100%

ART. 20 – Plataformas de validación de certificados electrónicos y de firma electrónica.

- Utilizar plataformas de validación de certificados electrónicos y de firma electrónica que garanticen lo establecido en el artículo 20. Tal es el caso de la plataforma @firma. 100%

Recuperación y conservación del Documento Electrónico: Cumplimiento Insuficiente

ART. 21 – Condiciones para la recuperación y conservación de los documentos.

- Definir y publicar la Política de gestión de documentos electrónicos de la entidad conforme a la NTI de Política de gestión de documentos electrónicos. (0%, no existe Archivero Municipal)
- Establecer un repositorio electrónico complementario y equivalente en su función a los archivos convencionales que contemple la aplicación de normas de conservación a los documentos depositados en él y su transferencia a otros repositorios. (0%)
- Establecer los calendarios de conservación de los documentos y expedientes electrónicos necesarios. (0%)
- Eliminar los documentos y expedientes electrónicos según la política de gestión de documentos electrónicos de la entidad, la normativa aplicable en materia de eliminación de Patrimonio Documental y aplicando las medidas de seguridad relacionadas definidas en el R.D. 3/2010 ENS. (0%)
- Generar documentos electrónicos conformes a la NTI de Documento electrónico. (50%, el gestor de expediente lo hace otras aplicaciones no)
- Intercambiar documentos electrónicos conforme a la NTI de Documento electrónico y mediante la estructura XML allí reflejada. (50%)
- Generar expedientes electrónicos conformes a la NTI de Expediente electrónico. (100%)
- Indizar o foliar cada expediente según lo dispuesto en la NTI de Expediente electrónico. (100%)
- Intercambiar expedientes electrónicos conforme a la NTI de Expediente electrónico y mediante la estructura XML allí reflejada. (100%, adaptado a INSIDE [9])
- Aprobar la normativa interna respecto a la atribución de la competencia en cuanto a la generación de copias auténticas tanto para la generación como la validación de las mismas. (0%)
- Asegurar el valor probatorio y la fiabilidad de los documentos electrónicos como evidencias electrónicas de las actividades a lo largo del tiempo. Por ejemplo a través de procesos de refirmado de documentos, uso de firma longeva, etc. (50%, sólo el gestor de expedientes)
- Establecer un esquema institucional de metadatos para la gestión interna del documento electrónico y conforme a la Política de gestión documental de la entidad. (0%)

Total cumplimiento: 37,5%

ART. 22 – Seguridad

- Aplicar el Esquema Nacional de Seguridad para garantizar la conservación de los documentos electrónicos. (0%)
- Cumplir con la normativa de protección de datos de carácter personal. (50%)
- Utilizar preferentemente firmas longevas que preserven la conservación de las firmas a lo largo del tiempo según lo dispuesto en la Política de firma de la entidad. (100%)

Total cumplimiento: 50%

ART. 23 – Formatos de los documentos.

- Conservar los documentos elaborados, enviados o recibidos en el formato original siempre que se garantice su preservación a lo largo del tiempo. (100%)
- Seleccionar formatos de documentos conformes con el artículo 11 y con la NTI de Catálogo de estándares. (100%)

- Aplicar procedimientos de copiado auténtico y conversión cuando exista riesgo de obsolescencia tecnológica del formato original. (0%)

Total cumplimiento: 66,66%

ART. 24 – Digitalización de documentos en soporte papel.

- Digitalizar los documentos en soporte papel de acuerdo a lo previsto en la NTI de Digitalización de documentos. 25%

Normas de conformidad: Cumplimiento insuficiente

ART. 27 – Mecanismos de control.

- Establecer los mecanismos de control que permitan verificar el cumplimiento del ENI en la entidad. 0%

ART. 28 – Publicación de conformidad.

- Publicación de la declaración de conformidad con el ENI y los posibles distintivos de interoperabilidad en la sede electrónica. 0% (Se activan en la sede cuando la administración cumple los anteriores artículos al completo)