Universitat Oberta de Catalunya

uoc.edu

Plan de adecuación al Esquema Nacional de Seguridad (ENS), para una administración pública local

Francisco Xabier Naveiro Cabanas
Máster Universitario en Ciberseguridad y Privacidad
Área de seguridad empresarial

Profesor colaborador: Iñaki Moreno Fernández
Profesora responsable de la asignatura: Cristina Romero Tris

Diciembre de 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Plan de adecuación al Esquema Nacional de Seguridad (ENS), para una administración pública local.*
Nombre del autor:	*Francisco Xabier Naveiro Cabanas*
Nombre del consultor/a:	*Iñaki Moreno Fernández*
Nombre del PRA:	*Cristina Romero Tris*
Fecha de entrega (mm/aaaa):	12/2021
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*M1.887 - TFM - Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*ENS, Riesgos, Ciberseguridad*

Resumen del Trabajo (máximo 250 palabras):

El proceso transformación digital de las Administraciones Públicas se ha desarrollado durante la última década de manera muy relevante, haciendo más intensivo el uso de las TI. Este proceso incrementa necesariamente la superficie de exposición a incidentes de seguridad, que ha de abordarse desde un punto de vista tecnológico y también normativo.

El desarrollo normativo en materia de Seguridad de la Información ha de favorecer un clima de confianza y en los sistemas de información y por consiguiente en los servicios prestados a través de la denominada Administración Electrónica.

El Esquema Nacional de Seguridad (ENS) es una norma de difícil cumplimiento por parte de las entidades locales de menor tamaño, dados sus escasos recursos tanto materiales como de personal y el desigual nivel de implantación de las TI. Para favorecer la implantación del ENS en este tipo de entidades es necesario poner en marcha mecanismos eficientes que proporcionen una serie de pautas para favorecer dicha implantación de forma práctica y homogénea, a la vez que proporcionan recursos a los que de otro modo no tendrían acceso.

En este Trabajo de Fin de Máster (TFM) se presenta la elaboración de un Plan de Adecuación al ENS para una entidad local de menos de 5.000 habitantes, utilizando mecanismos y herramientas que faciliten la consecución de ese objetivo en el contexto de cooperación y desarrollo de la Administración Local. Con este pretexto también se analiza la futura evolución de la norma del ENS, a la luz del anuncio publicado sobre su inminente actualización.

Abstract (in English, 250 words or less):

The digital transformation process of Public Administrations has developed during the last decade in a very relevant way, making the use of IT more intensive. This process necessarily increases the surface of exposure to security incidents, which must be addressed from a technological and also regulatory point of view.

The normative development in the matter of Information Security has to favor a climate of trust and in the information systems and consequently in the services provided through the so-called Electronic Administration.

The National Security Scheme (ENS) is a standard that is difficult to comply with by smaller local entities, given their scarce material and personnel resources and the uneven level of IT implementation. In order to favor the implementation of the ENS in this type of entity, it is necessary to put in place efficient mechanisms that provide a series of guidelines to favor said implementation in a practical and homogeneous way, at the same time that they provide resources to which they would not otherwise have access.

In this Master's Thesis (TFM), the preparation of an Adaptation Plan to the ENS is presented for a local entity with less than 5,000 inhabitants, using mechanisms and tools that facilitate the achievement of this objective in the context of cooperation and development of Local Administration. With this pretext, the future evolution of the ENS standard is also analyzed, in light of the announcement published about its imminent update.

Índice

Lista de figuras

Lista de tablas

1 Introducción

1.1 Contexto y justificación del Trabajo

El proceso de normativizar la Seguridad de la Información en las Administraciones Públicas transcurre en paralelo a la necesaria transformación digital de las mismas hacia la denominada administración electrónica.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) [1] es la primera norma que reconoce a los ciudadanos su derecho a relacionarse electrónicamente con las administraciones públicas y, por consiguiente, la obligación de éstas a garantizar ese derecho. En el Art. 42.2 recoge el objeto del Esquema Nacional de Seguridad (ENS).

> **Ley 11/2007, de 22 de junio. Art. 42.2.**
> El **Esquema Nacional de Seguridad** tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Con igual literalidad se identifica también la finalidad del **Esquena Nacional de Seguridad** (ENS) en la Ley 40/2015, de 1 de octubre, de régimen jurídico del Sector Público [2], en su Art. 156.2.

La Ley 11/2077 es, pues, referencia inicial en esta materia, si bien ya ha sido derogada con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b de la Ley 39/2015, de 1 de octubre [3].

Es interesante señalar que hay un ámbito de la administración, el de la justicia, que posee características que la diferencian de las otras Administraciones públicas, y es por ello que impulsa ese mismo proceso de transformación digital apoyándose en una norma singular, la ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. Lo que en el contexto de las Administraciones Públicas se articuló por medio del Esquema Nacional de Seguridad (ENS), en el ámbito de la Administración de Justicia se condujo por la vía del del denominado Esquema judicial de interoperabilidad y seguridad (EJIS).

El ENS se regula por primera vez en el Real Decreto 3/2010, de 8 de enero [4]. Posteriormente, el Real Decreto 951/2015, de 23 de octubre, de modificación del anterior RD [5] establece, entre otras cuestiones, que los sistemas deberán adecuarse a lo dispuesto en un plazo de veinticuatro meses (5 de noviembre de 2017).

El desarrollo normativo que acompaña al proceso de transformación digital de las Administraciones Públicas tiene continuidad en la Ley 39/2015 mencionada anteriormente, que en su artículo 13 identifica los derechos de las personas en sus relaciones con estas.

El RD 3/2010 que regula el ENS tiene ya 11 años, y aun cuando fue actualizado por el RD 951/2015, aspectos tan relevantes como el avance en la transformación digital de las administraciones públicas, la intensificación de las amenazas y los incidentes de seguridad, las evoluciones tecnológicas de los últimos años, e incluso el aprovechamiento de los conocimientos adquiridos en ciberseguridad y ciberinteligencia, hacen necesaria su revisión.

En el mes de junio de 2021 se ha publicado por parte del Ministerio de Asuntos Económicos y Transformación Digital el **proyecto de un nuevo real decreto por el que se regulará el ENS y que sustituirá el actual RD 3/2010** [6].

La pretensión que se plantea en este TFM es la de elaborar un **Plan de adecuación al Esquema Nacional de Seguridad (ENS) para una administración pública local**, toda vez que entre las entidades obligadas a adoptar el ENS están las que integran la Administración Local.

Se ha escogido como entidad objetivo un **ayuntamiento ficticio de menos de 5.000 habitantes** que decide abordar la implantación y posterior certificación de cumplimiento del ENS adhiriéndose a la estrategia de certificación puesta en marcha por un organismo superior, la Diputación Provincial, que actuará como entidad certificadora. Esta elección obedece al interés por favorecer la adecuación al ENS de un gran número de organizaciones, las entidades locales más pequeñas, que por lo general mantienen una disponibilidad de recursos escasa, tanto desde el punto de vista presupuestario como de personal.

1.2 Objetivos del Trabajo

El objetivo principal de este TFM es la **elaboración de un plan para la adecuación al ENS de una Administración Pública local de menos de 5.000 habitantes**, teniendo en consideración para ello un marco de trabajo basado en la coordinación dentro de un convenio con el organismo superior (Diputación Provincial), y además aplicando Perfiles Específicos de Cumplimiento a los pueden acogerse las Entidades Locales (EELL), siendo entonces de aplicación la declaración de aplicabilidad asociada a un perfil en concreto, en nuestro caso, el definido en **CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (menos de 5.000 habitantes)** [7].

A la hora de elaborar este TFM, la evolución del marco normativo viene definida por el borrador del proyecto de un nuevo real decreto por el que se regulará el ENS, que ha sido publicado en el mes de junio de este año, y que sustituirá el actual RD 3/2010. Como objetivo derivado de lo anterior, se **revisarán los cambios que introduce este borrador en la reglamentación de seguridad ENS**.

1.3 Enfoque y método seguido

Según se recoge en el ENS, dicho esquema se plantea con la finalidad de **crear las condiciones necesarias de confianza en el uso de los medios electrónicos**, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Tal y como define el Art. 3 del RD 3/2010, las entidades locales están incluidas en el ámbito de aplicación de dicha norma, por lo que han de llevar a cabo las actuaciones necesarias para adecuar sus sistemas para el cumplimento del ENS. En definitiva, han de implantar el proceso de seguridad en su organización con una gestión continuada de la misma.

En los ayuntamientos de menos de 5.000 habitantes se precisará abordar la adecuación al ENS siguiendo las mismas fases requeridas para corporaciones de mayor tamaño, aunque con las correspondientes adaptaciones, dada la limitación de recursos de las entidades más pequeñas:

- **Fase I – Elaboración del Plan de Adecuación**.
- Fase II – Implementación del Plan de Adecuación.
- Fase III – Conformidad con el ENS.
- Fase IV – Evaluación y mejora continua (auditoría)

Este TFM se ocupa exclusivamente de la Fase I. Para incluir los sistemas en la gestión de la seguridad de la información y las comunicaciones de manera alineada con el ENS, en este TFM se llevan a cabo las siguientes actividades:

- **Identificación de los sistemas de información**. Se identifica la Información que se maneja y los Servicios que se utilizan, lo que da lugar a la relación de los Sistemas de Información objeto del Plan de Adecuación.
- **Categorización del sistema**. Valoración de las dimensiones de seguridad y categorización de los Sistemas de acuerdo al Anexo I del ENS y apoyándose en la guía *CCN-STIC 803 Valoración de los sistemas* [8] y *CCN-STIC 883 Implantación del ENS para Entidades Locales* [9].
- **Análisis de riesgos de los sistemas de información**. Para el análisis de riesgos se utiliza la metodología Megerit v3. Se ha empleado la aplicación PILAR recomendada por el CCN para llevarlo a cabo. El análisis ha incluido las siguientes tareas:
    - Modelado en PILAR del Sistema de Información y los activos a analizar. Se han categorizado los activos e identificado las dependencias entre ellos.
    - Identificación y valoración de las amenazas en función de la categoría de los activos.
    - Selección de las salvaguardas a aplicar según la categoría del sistema de acuerdo al Anexo II del ENS y valoración del nivel de madurez en cuanto al cumplimiento de las mismas.
    - Determinación del riesgo residual resultante.
- **Plan de mejora de la seguridad**. Definición de un plan de mejora con la identificación de las acciones a llevar a cabo en cada fase del proyecto de adecuación para alcanzar la situación objetivo a partir del análisis de la situación actual.

1.4 Planificación del Trabajo

1.4.1 Diagrama Gantt

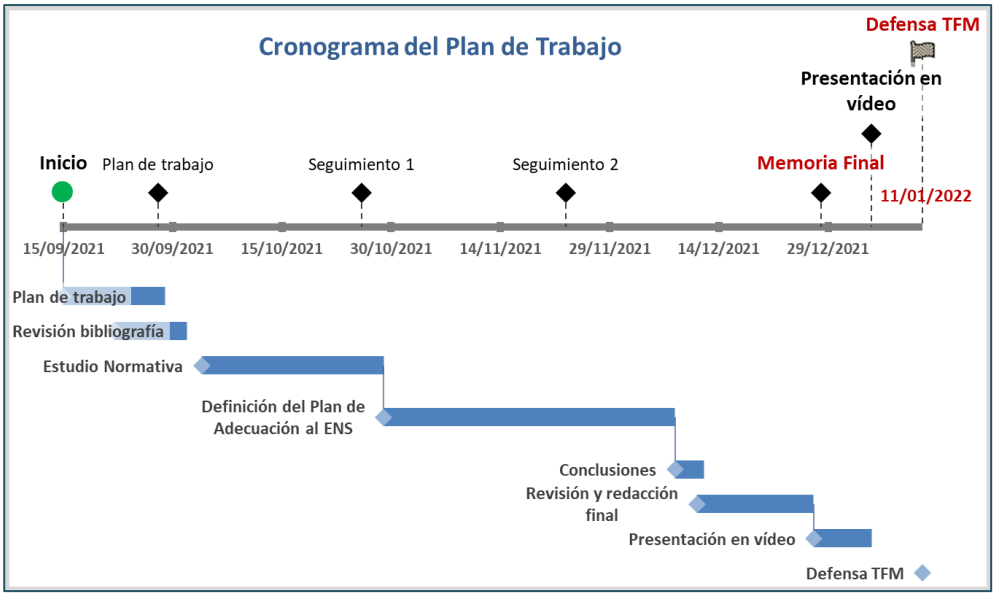


Ilustración 1 Diagrama Gantt del plan de trabajo

1.4.2 Tareas

Tarea	Inicio	Fin	Duración	Descripción
1	**15/09/2021**	**28/09/2021**	**14**	**Plan de trabajo**
2	**22/09/2021**	**01/10/2021**	**10**	**Revisión bibliografía**
3	**04/10/2021**	**28/10/2021**	**25**	**Estudio Normativa**
3.1	04/10/2021	13/10/2021	10	Revisión normas vigentes y su evolución
3.2	04/10/2021	23/10/2021	20	Estudio del ENS y guías técnicas asociadas
3.3	14/10/2021	26/10/2021	13	Análisis de los cambios en el borrador del RD nuevo ENS
3.4	24/10/2021	28/10/2021	5	Identificación del impacto de los cambios
4	**29/10/2021**	**07/12/2021**	**40**	**Definición del Plan de Adecuación al ENS**
4.1	29/10/2021	07/11/2021	10	Política de seguridad y normativa interna
4.2	08/11/2021	02/12/2021	25	Identificación de los servicios y categorización de sistemas de información
4.3	30/11/2021	02/12/2021	3	Determinación de la Declaración de Aplicabilidad provisional
4.4	31/10/2021	04/12/2021	35	Análisis de Riesgos
4.5	05/12/2021	07/12/2021	2	Elaboración de la Declaración de Aplicabilidad definitiva
5	**08/12/2021**	**11/12/2021**	**4**	**Conclusiones**
6	**11/12/2021**	**26/12/2021**	**16**	**Revisión y redacción final**
7	**27/12/2021**	**03/01/2022**	**8**	**Presentación en vídeo**
8		**11/01/2022**	**1**	**Defensa TFM**

Tabla 1 Tareas del Plan de Trabajo del TFM.

1.4.3 Hitos

Fecha	Hito
15/09/2021	**Inicio**
28/09/2021	**Plan de trabajo**
26/10/2021	**Seguimiento 1**
23/11/2021	**Seguimiento 2**
28/12/2021	**Memoria Final**
04/01/2022	**Presentación en vídeo**
11/01/2022	**Defensa TFM**

Tabla 2 Hitos del Plan de Trabajo del TFM.

2 El Esquema Nacional de Seguridad (ENS)

2.1 Introducción al ENS

Las Administraciones Públicas (AAPP) deben servir a los intereses generales y regirse por el principio de la eficacia, lo que inherentemente las obliga usar las **Tecnologías de la Información** para prestar sus servicios a los ciudadanos. Estamos hablando, pues, de la **Administración Electrónica** y de garantizar el acceso de los ciudadanos y entidades a los servicios de la administración por medios electrónicos, lo que da origen a la Ley 11/2007 [1], ya derogada con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre [3].

Para cumplir con este mandato, las Administraciones Públicas necesariamente han de disponer de los procesos y herramientas más adecuadas que garanticen, no solo la efectividad de sus procedimientos, sino la **seguridad y confiabilidad** de sus actuaciones. Por ello se elabora la norma del Esquema Nacional de Seguridad (ENS), viene establecido de origen en el Art. 42 de la Ley 11/2007 [1], y está regulado en el RD 3/2010 [4], posteriormente actualizado por el RD 951/2015 [5].

El ENS establece los principios básicos y los requisitos mínimos de seguridad de los Sistemas de Información de las Administraciones Públicas.

> **Artículo 4. Principios básicos del Esquema Nacional de Seguridad.**
> El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información.

En los siguientes apartados se lleva a cabo un examen de los contenidos del ENS y su organización, así como de la evolución prevista para adaptarse a los cambios normativos, tecnológicos y a un creciente nivel de las amenazas a las que se ven sometidos los sistemas de información de las AAPP.

2.2 Estructura y Contenido

En el presente apartado se examina de manera resumida el contenido del RD 3/2010, describiendo los capítulos que lo integran y sus anexos.

La norma se estructura en **diez capítulos**, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria y tres disposiciones finales. Además, se completa con **cinco anexos** dedicados a la **categoría de los sistemas**, las **medidas de seguridad**, la **auditoría de la seguridad**, el glosario de términos y un último anexo con un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes.

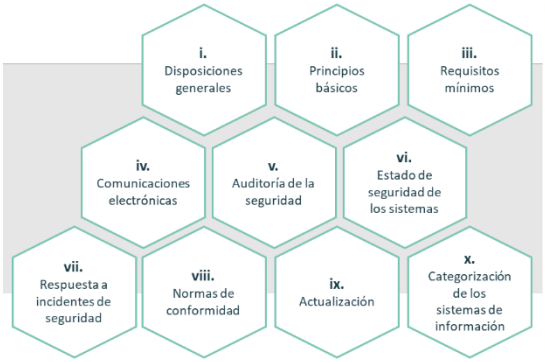


Ilustración 2 Capítulos del ENS

2.2.1 Capítulos del ENS

i. Disposiciones Generales.

Contiene el objeto y ámbito de aplicación. Se incluyen todas las Administraciones Públicas indicadas en el Art. 2 de la Ley 11/2007, entre las que se encuentran las entidades que integran la **Administración Local**. Se excluye expresamente de su ámbito de aplicación los sistemas que tratan información clasificada.

ii. Principios básicos.

Enumera y explica los seis principios básicos para asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información con seguridad: **Seguridad integral**, **Gestión de Riesgos**, **Prevención reacción y recuperación**, **Líneas de defensa**, **Reevaluación periódica** y **Función diferenciada**.

Define la **seguridad como un proceso integral** en el que no solo se han de incluir los elementos técnicos sino también las **personas** que se relacionan con los sistemas.

Formula la **gestión de los riesgos** como piedra angular de la gestión de la seguridad, que a su vez ha de estar sometida a un proceso de mejora continua.

iii. Requisitos mínimos

Establece la obligatoriedad para las Administraciones Públicas de disponer de una **Política de Seguridad** basada en los principios básicos introducidos en el capítulo 2, y además enumera y detalla los **requisitos mínimos** que han de permitir el desarrollo de dicha política:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.

h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

No todos ellos serán siempre de obligado cumplimiento, sino que han de exigirse de manera proporcional a los riesgos identificados para cada sistema.

Los municipios podrán acogerse a una **política de seguridad común** elaborada por el organismo superior, Diputación u órgano análogo.

iv. Comunicaciones electrónicas

Se reconoce al ENS como la norma de aplicación en cuanto a la seguridad de las comunicaciones electrónicas y firma electrónica, esta última de acuerdo con lo que establece el Esquena Nacional de Interoperabilidad (ENI) acerca de la política de firma y de certificados.

v. Auditoría de la seguridad

Establece los diferentes niveles de auditoría de la seguridad de TI, en tanto en cuanto las Administraciones Públicas dentro del ámbito del ENS han de implantar la gestión de la seguridad de la información sujeta a un proceso cíclico de mejora continua, para lo cual las auditorías resultan imprescindibles.

vi. Estado de seguridad de los sistemas

Declara el objetivo de disponer de un **perfil general del estado de la seguridad en las Administraciones públicas**, para lo cual otorga al Comité Sectorial de Administración Electrónica la competencia de organizar y articular el procedimiento de recogida de la información necesaria para la consecución del Informe Nacional sobre el Estado de la Seguridad (INES).

vii. Respuesta a incidentes de seguridad

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada **CCN-CERT** (Centro Criptológico Nacional-*Computer Emergency Reaction Team*).

Dentro de su proceso de respuesta a incidentes de seguridad, cada entidad pública debe incluir el traslado de información al CCN-CERT de los incidentes más graves.

El CCN-CERT asume igualmente la tarea de informar sobre **vulnerabilidades, alertas y avisos de nuevas amenazas**, así como la **formación en materia de seguridad** al personal de las Administraciones Públicas.

viii. Normas de conformidad

Las sedes y registros electrónicos son el mecanismo fundamental de acceso de los ciudadanos y entidades a la Administración Electrónica, y su seguridad ha de

regirse por lo establecido en el ENS. Además, los órganos de las Administraciones Públicas han de mostrar en sus sedes el cumplimiento con el ENS a través de la publicación de sus declaraciones de conformidad, que incluirán tres cuerpos: Identificación del declarante, contenido de la declaración y justificación de la conformidad.

Por otro lado, las especificaciones de seguridad han de formar parte de todo el ciclo de vida de los servicios y sistemas, ya desde su mismo diseño, a través de los procedimientos de control adecuados en cada caso.

ix. Actualización

El ENS, como modelo de organización de la seguridad de los sistemas de información de las Administraciones Públicas, ha de mantenerse actualizado permanentemente.

Su actualización será imperativa para adaptarse al necesario progreso de la Administración Electrónica, a la evolución tecnológica y normativa, así como a nuevos estándares en seguridad y auditoría de los sistemas y tecnologías de la información.

En el apartado 2.3 Actualización del ENS, se detalla la evolución prevista en la fecha de elaboración de este TFM.

x. Categorización de los sistemas de información

Los sistemas de información habrán de categorizarse en función del impacto que tendría un incidente que afectase a la seguridad de los servicios o de la información que manejan en cualquiera de las dimensiones de la seguridad definidas en el Anexo I del ENS.

La categorización de un sistema deberá atender al principio de proporcionalidad, modulando el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto.

2.2.2 Anexos del ENS

Anexo I. Categorías de los sistemas

La categorización de la seguridad de un sistema se llevará a cabo en función del impacto que tendría un incidente que afectase a la seguridad de la información o los servicios en cualquiera de las dimensiones de seguridad.

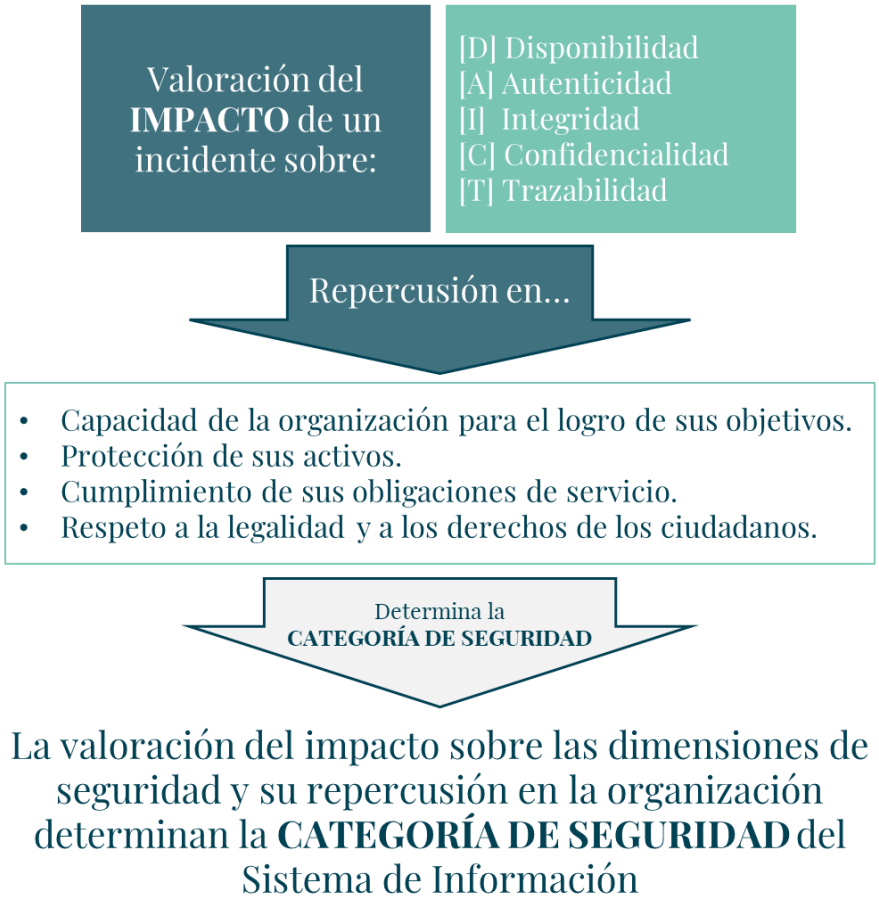


Ilustración 3 Determinación de la categoría de seguridad del sistema de información.

Para el análisis y categorización de un Sistema de Información se deben evaluar las cinco dimensiones de seguridad:

- **Disponibilidad (D)**: los activos han de estar accesibles para los usuarios, entidades o procesos autorizados cuando lo requieran.
- **Autenticidad (A)**: una entidad es quien dice ser o bien garantiza la fuente de la que proceden los datos.
- **Integridad (I)**: el activo de información no ha sido alterado de manera no autorizada.
- **Confidencialidad ©**: la información solo se pone a disposición de entidades o procesos autorizados.
- **Trazabilidad (T)**: las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad, lo que deriva en la condición de no repudio de las mismas.

La **eficacia jurídica** de los procedimientos administrativos depende de que se garanticen las dimensiones anteriores.

Un sistema de información y, en consecuencia, los servicios que ofrece y la información que maneja, puede ser afectado en una o más dimensiones de seguridad. El ENS define que a cada dimensión de la seguridad afectada por un incidente se le asignará uno de los siguientes niveles: **BAJO**, **MEDIO** o **ALTO**. Si una dimensión no se ve afectada no se le asignará ninguno de los niveles.

- **Nivel BAJO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio limitado** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

  Se entenderá por **perjuicio limitado**:

  1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

  2.º El sufrimiento de un daño menor por los activos de la organización.

  3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

  4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

  5.º Otros de naturaleza análoga.

- **Nivel MEDIO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio grave** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

  Se entenderá por **perjuicio grave**:

  1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

  2.º El sufrimiento de un daño significativo por los activos de la organización.

  3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

  4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.

  5.º Otros de naturaleza análoga.

- **Nivel ALTO**: Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio muy grave** sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados

  Se entenderá por **perjuicio muy grave**:

  1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.º El incumplimiento grave de alguna ley o regulación.

4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.º Otros de naturaleza análoga.

En función de la valoración efectuada de las dimensiones de la seguridad de un sistema de información, este se categorizará en una de las siguientes **CATEGORÍAS**:

- Categoría **ALTA**: si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- Categoría **MEDIA**: si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
- Categoría **BÁSICA**: si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Cuando un sistema maneje diferentes informaciones y preste diversos servicios, **el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio**.

En resumen, la secuencia de actuaciones para determinar la categoría de un sistema de información es la siguiente:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad.
2. Determinación de la categoría del sistema, según el nivel máximo alcanzado en la valoración de cada una de sus dimensiones de seguridad.

Anexo II. Medidas de seguridad

Las **Medidas de Seguridad**, también denominadas ***controles*** o ***salvaguardas***, son un conjunto de disposiciones orientadas a protegerse de los posibles riesgos sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad.

En función del momento en que se apliquen, pueden tener carácter **preventivo** y **disuasorio**. Pueden ser medidas de **protección ante vulnerabilidades** identificadas en los sistemas. Pueden ser empleadas para la **detección de los incidentes de seguridad** y la consecuente adopción de la **reacción** adecuada. Por último, también pueden establecerse medidas de **recuperación**, para cuando haya ocurrido un incidente y el sistema deba ser devuelto a su estado anterior al impacto.

El ENS divide las medidas de seguridad en tres grupos:

a) Organizativas [org]. Se refieren a la organización global de la seguridad.

b) Operacionales [op]. Relativas a la protección de la operación del sistema (accesos, explotación, servicios externos, continuidad, etc.).

c) De protección [mp]. Enfocadas a proteger activos concretos (instalaciones, equipos, comunicaciones, etc.).

Es necesario determinar cuáles de las medidas son de aplicación al sistema de información en concreto que se pretende proteger, puesto que no todas ellas han de emplearse en todos los casos, sino que se seleccionan en función de la categorización previa que se haya realizado sobre el sistema, y teniendo en consideración la probabilidad real que pueda existir de que un incidente afecte al activo que se protege.

La relación de las medidas que se hayan seleccionado para proteger el Sistema de Información se denomina **Declaración de Aplicabilidad**, y constituye un documento básico dentro del proceso de adecuación al ENS.

En nuestro caso concreto, al menos en una primera fase se aplicarán únicamente los controles definidos en el **perfil de cumplimiento específico para ayuntamientos de menos de 5.000 habitantes** (Tabla 16).

Anexo III. La auditoría de seguridad

El objeto de la auditoría de seguridad es verificar el cumplimiento del ENS, y en consecuencia emitir un informe basado en la evidencia del grado de cumplimiento de las medidas de seguridad. También deberán identificarse las deficiencias y sugerir medidas correctoras para alcanzar el cumplimiento establecido según la categoría del sistema.

La auditoría, en caso de tener resultado positivo, posibilita la obtención del certificado de conformidad con el ENS.

El marco de las auditorías en el contexto del ENS viene definido en el Art. 34 y Anexo III del RD 3/2010, que establece dos tipos:

- **Auditoría regular ordinaria**: a realizar al menos cada dos años, es obligatorio hacerla a los sistemas de categoría MEDIA o ALTA, incluyendo los de empresas que presten servicios a las Administraciones Públicas dentro del ámbito de aplicación del ENS.

  Con carácter extraordinario, deberá realizarse antes de dos años si se produce una modificación relevante del Sistema de Información que pueda repercutir en las medidas de seguridad requeridas.

  En el caso de los sistemas de categoría ALTA, en función de los hallazgos plasmados en el informe de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, hasta la subsanación de las deficiencias identificadas.

- **Autoevaluación de las medidas aplicables**: Para los sistemas de categoría BAJA no es obligado realizar una auditoría formal, basta con una **autoevaluación** realizada simplemente por los propios administradores del sistema, sin intervención de ninguna entidad auditora externa.

Anexo III del RD 3/2010 señala en qué términos deben ser auditados los sistemas de información en el contexto del ENS:

a) Que la **política de seguridad** define los **roles** y **funciones** de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
b) Que existen procedimientos para **resolución de conflictos** entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de "**separación de funciones**".
d) Que se ha realizado un **análisis de riesgos**, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre **Medidas de Seguridad**, en función de las condiciones de aplicación en cada caso.
f) Que existe un **sistema de gestión de la seguridad de la información**, documentado y con un proceso regular de aprobación por la dirección.

2.3 Actualización del ENS

2.3.1 Modificaciones derivadas del RD 951/2015

Como ya se ha mencionado anteriormente, el RD 951/2015 [5] introdujo algunas modificaciones en el ENS, fruto del análisis llevado a cabo durante la implantación en una serie de entidades y teniendo también en consideración la evolución tecnológica y las nuevas amenazas identificadas desde la entrada en vigor del RD 3/2010, de 8 de enero.

De manera resumida, los cambios más relevantes introducidos en el ENS fueron:

- Se enumeran las siguientes Instrucciones Técnicas de Seguridad, de obligado cumplimiento para las Administraciones Públicas dentro del ámbito del ENS:
    a) Informe del estado de la seguridad.
    b) Notificación de incidentes de seguridad.
    c) Auditoría de la seguridad.
    d) Conformidad con el Esquema Nacional de Seguridad.
    e) Adquisición de productos de seguridad.
    f) Criptología de empleo en el ENS.
    g) Interconexión en el Esquema Nacional de Seguridad.
    h) Requisitos de seguridad en entornos externalizados.
- Se incorpora la obligatoriedad de adecuación de los sistemas de identificación electrónica a lo previsto en el Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014 [10].
- Se actualizan una serie de medidas de seguridad recogidas en el Anexo II del ENS, entre las que destacan:
    - [op.acc.5]; obligación de un mecanismo de autentificación basado en doble factor para los sistemas de nivel MEDIO.

    - [op.exp.8]; obligación de registrar las actividades de los usuarios también en los sistemas de niveles BAJO y MEDIO.
    - [op.mon.1]; extensión de la obligación de disponer de herramientas de detección o de prevención de intrusión a los sistemas de nivel MEDIO.
    - [po.mon.2]; los sistemas de niveles BÁSICO y MEDIO también han de ser monitorizados, en función de su categoría.
    - [mp.si.5]; aplicación de la medida de borrado seguro de soportes de información también a los sistemas de nivel BAJO.
    - [mp.info.9]; las copias de seguridad han de realizarse en los sistemas de todos los niveles: BAJO, MEDIO o ALTO.
- Se introduce la necesidad de formalizar la **Declaración de Aplicabilidad**.
- Se detalla la función del CCN-CERT en cuanto a la coordinación en materia de seguridad de los sistemas de información (incidentes de seguridad, estado de implantación del ENS en las AAPP, etc.).

2.3.2 Proyecto de nuevo Real Decreto del ENS

En el mes de junio de 2021 el Ministerio de Asuntos Económicos y Transformación Digital ha publicado el proyecto de un nuevo Real Decreto [6] por el que se regulará el ENS y que sustituirá el actual RD 3/2010.

Desde la última actualización del ENS en el año 2015, se ha acelerado de manera sostenida la digitalización de la sociedad en general y de las AAPP en particular, lo que ha propiciado un aumento en la superficie de exposición y un notable incremento de los ciberataques, que además de causar daños en los activos, socavan la confianza en las tecnologías de la información. El sector público no es ajeno a este contexto y a menudo es el objetivo de dichos ataques.

En un escenario como el actual, de manera global muchos gobiernos reaccionan impulsando la puesta en marcha o la actualización de sus respectivos arsenales normativos, programas y medidas en materia de seguridad de la información y las comunicaciones, como es el caso de EEUU, con la reciente promulgación de la *Executive Order on Improving the Nation's Cybersecurity*.

El Gobierno de España también está promoviendo un conjunto de medidas urgentes en materia de ciberseguridad por acuerdo del Consejo de Ministros:

1. Plan de choque de ciberseguridad
2. **Actualización del ENS mediante tramitación urgente**
3. Promoción e incentivación de la adopción de sistemas, estándares y políticas de gestión de la seguridad en el sector privado.

Desde esta perspectiva, los **elementos que impulsan la actualización del ENS** según indican Javier Candau (CCN) y Miguel Ángel Amutio (SGAD) en el III Encuentro ENS celebrado en junio de 2021 [11] son, entre otros:

- El progreso de la transformación digital.
- La intensificación de los ciberataques.
- Avance de las tecnologías.

- Evolución del marco legal.
- Mejor conocimiento del estado de la seguridad (INES).

Entre los objetivos que se plantean conseguir con la actualización del ENS se resaltan en el siguiente cuadro.

Objetivo 1: Mejorar y alinear el ENS

- Actualizar referencias al **marco legal**.
- Precisar el **ámbito de aplicación**, ampliando al sector privado que presta servicios a las Administraciones Públicas e incluyendo los sistemas que manejan información clasificada.
- Precisar las condiciones y actuaciones en relación a la **prevención**, **detección** y **respuesta a incidentes**.

Objetivo 2: Capacidad de ajustar requisitos

- Introducción de los **perfiles de cumplimiento específico**, como conjuntos de medidas de aplicación a necesidades concretas, como por ejemplo las entidades locales.

Objetivo 3: Revisar principios, requisitos y medidas

- **Principios**: Mejora de la respuesta y **diferenciación de responsabilidades**. Se hace foco en los términos y conceptos de **respuesta**, **conservación**, **vigilancia continua**. También se adapta el principio de **diferenciación de responsabilidades**.
- **Requisitos**: La seguridad por defecto se denominará "***mínimo privilegio***".
- **Medidas**: se **actualizan las medidas del Anexo II** y aparece una nueva familia de Servicios en la nube. También se revisa la codificación de los requisitos y los refuerzos.

2.3.2.1 Principales novedades en el proyecto de nuevo RD del ENS

Según consta en la *Memoria del análisis de impacto normativo del proyecto de real decreto por el que se regula el esquema nacional de seguridad* [12], entre las principales novedades que aporta este proyecto de RD sobre el actual se encuentran las siguientes:

- **Ámbito de aplicación:**
  1º. Clarificación con la finalidad de concienciar al sector público y privado de lo que les es exigible en materia de ciberseguridad.
  2º. Extender la aplicación del ENS a los sistemas que manejan información clasificada, que en el anterior RD se habían quedado al margen.
- **Comunicaciones electrónicas;** Se ha eliminado completamente el capítulo IV Comunicaciones electrónicas, al ser superado por las leyes 39/2015 [3] y 40/2015 [2] y sus desarrollos reglamentarios.
- **Perfiles de cumplimiento específico;** En el art. 30 se incorporan los perfiles de cumplimiento específico, que introducen la capacidad de ajustar los requisitos del ENS a necesidades específicas, y que, como veremos a lo largo de este TFM, son relevantes para el caso de las entidades locales.
- **Principios básicos:**

1º. El principio antes denominado ‘prevención, reacción y recuperación’ pasa a denominarse ‘**prevención, detección y respuesta’**.

2º. Se introduce el principio ‘**vigilancia continua**’ para permitir la detección de actividades o comportamientos anómalos y su oportuna respuesta e impulsar la **evaluación permanente** del estado de la seguridad de los activos.

3º. Se clarifica la redacción del principio ‘**responsabilidades diferenciadas**’ para precisar los aspectos relativos al responsable de la seguridad y al responsable del sistema. Se diferencian cuatro roles:

- Responsable de información
- Responsable del servicio
- Responsable de la seguridad
- Responsable del sistema

- **Política de seguridad y requisitos mínimos de seguridad;** principalmente se refuerzan la importancia de la **política de seguridad** y el requisito mínimo ‘seguridad por defecto’ que pasa a denominarse ‘**mínimo privilegio**’.

  Para los servicios externalizados, se crea la nueva figura de **POC** (Punto o Persona de Contacto) de Seguridad de la información, que será el propio responsable de seguridad de la organización contratada o formará parte de su área o tendrá comunicación directa con la misma.

- **Prevención, detección y respuesta a incidentes.** Se detallan de forma más pormenorizada en este capítulo:

  1º. Las condiciones relativas a la notificación de incidentes de seguridad por parte de las entidades del sector público al CCN-CERT y a las correspondientes actuaciones de respuesta por parte de la Secretaría General de Administración Digital y del CCN-CERT.

  2º. Las condiciones de la notificación de incidentes de seguridad al INCIBE-CERT por parte de las entidades del sector privado que preste servicios a las entidades públicas; todo ello en el marco de lo previsto en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [13].

- **Medidas de seguridad** (Anexo II); se han actualizado las medidas de seguridad en el **marco operacional [op]** y en las **medidas de protección [mp]**. Más adelante, en este documento, se detallarán las actualizaciones que contiene el proyecto de nuevo RD en esta área.

En el contexto de este TFM, es preciso resaltar la intención de incluir en el nuevo RD los **perfiles de cumplimiento específico**, que hasta el momento actual solo se manejan como instrumento de implementación, es decir, de carácter práctico, y principalmente enfocado a entidades locales (ver, por ejemplo, *CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (<5.000 habitantes)* [7]), pero que en el nuevo ENS toman carta de naturaleza.

Lo que se pretende con este recurso es la capacidad de ajustar los requisitos del ENS para que, en virtud del principio de proporcionalidad y procurando una adaptación al ENS más eficaz y eficiente, se adecuen a entidades o sectores concretos, atendiendo

a los riesgos a los que están expuestos sus sistemas de información y servicios. Estos perfiles específicos serán validados y publicados por el CCN.

También se formula el concepto de **esquemas de acreditación de entidades y validación de personas**, pensados para la implantación y configuración de soluciones o plataformas suministradas por terceros con las garantías de seguridad exigibles en cada caso.

2.3.2.2 Detalle de modificaciones del Anexo II

En el proyecto del nuevo RD del ENS se propone una actualización de las medidas de seguridad en el marco operacional y en las medidas de protección. Algunas medidas amplían notablemente su nivel de exigencia para determinadas categorías y otras lo incrementan levemente. En sentido contrario, algunas medidas ven simplificado su nivel de exigencia, e incluso algunas se eliminan o se engloban dentro de otras. También se han creado algunas medidas nuevas.

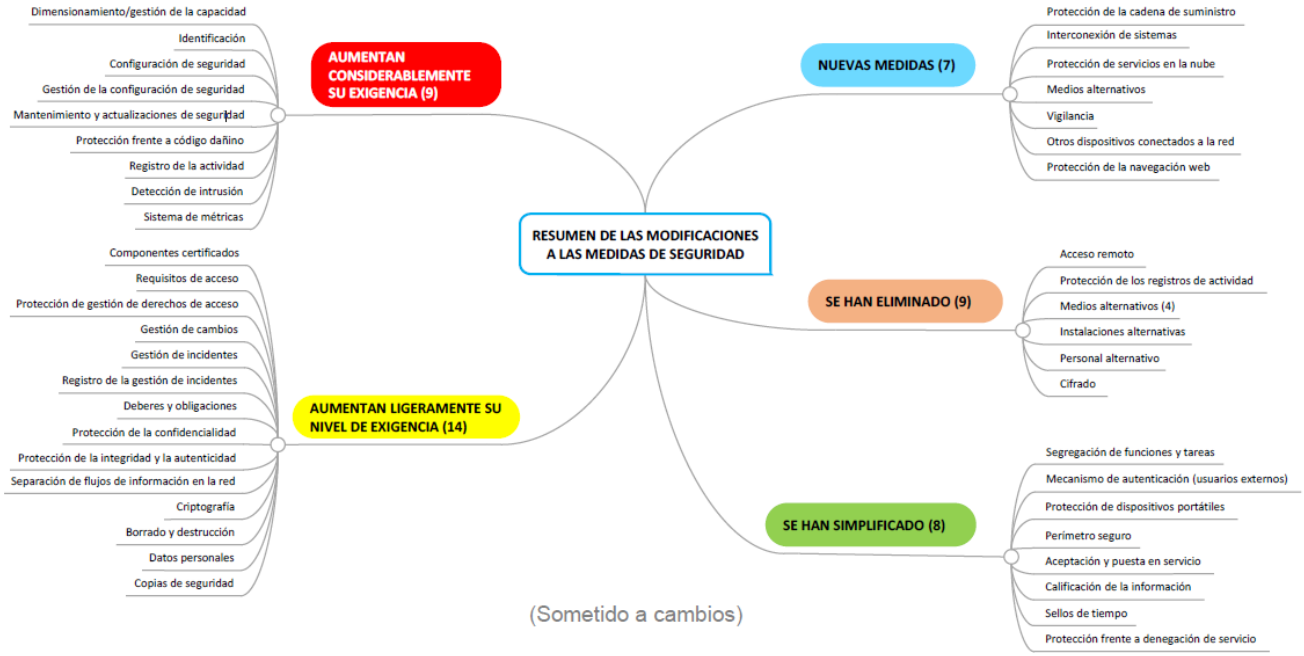


Ilustración 4 Panorámica de evolución de las medidas de seguridad. (Fuente: [11])

A continuación, se revisan en detalle los cambios propuestos en los controles, tanto en los del marco operacional [op] como en las medidas de protección [mp].

Marco operacional:
PLANIFICACIÓN ✓ Se refuerza significativamente la exigencia en la arquitectura de seguridad y en el dimensionamiento/gestión de la capacidad. **CONTROL DE ACCESO** ✓ Se incrementan significativamente los requisitos de identificación.

- ✓ Se refuerzan levemente los requisitos de acceso y la protección de gestión de derechos de acceso.
- ✓ Se aligeran las exigencias en materia de segregación de tareas.

EXPLOTACIÓN

- ✓ Reforzadas significativamente en la configuración de seguridad y su gestión, mantenimiento y actualizaciones de seguridad, la protección frente a código dañino y el registro de la actividad de los usuarios.
- ✓ Aumenta moderadamente su exigencia en gestión de cambios e incidentes (se exige desde categoría BÁSICA).
- ✓ Se elimina el control relativo a la protección de los registros de actividad, ya contemplado en otras medidas.

RECURSOS EXTERNOS

- ✓ Se incorporan nuevas medidas destinadas a los recursos externos provistos, cada vez más frecuentes en la administración digital: protección de la cadena de suministro, interconexión de sistemas.

CONTNUIDAD DEL SERVICIO

- ✓ Se incorpora medios alternativos (que engloba todas las referentes a personal, equipos, instalaciones… alternativas que se han eliminado de las medidas de protección).

SERVICIO EN LA NUBE

- ✓ Se introduce una nueva medida para la protección de servicios en la nube.

MONITORIZACIÓN DEL SISTEMA

- ✓ Se ha reforzado significativamente la exigencia de las medidas de detección de intrusión y sistema de métricas
- ✓ Se ha incorporado una nueva medida de vigilancia, alentada por las más recientes prácticas internacionales, dirigida a asegurar el mantenimiento de la monitorización constante de la seguridad del sistema.

Medidas de protección:

PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

- ✓ Se han realizado cambios editoriales y eliminado las instalaciones alternativas

GESTIÓN DEL PERSONAL

- ✓ Se ha incrementado levemente la exigencia en deberes y obligaciones y eliminado personal alternativo.

PROTECCIÓN DE LOS EQUIPOS

- ✓ Se incorpora nueva medida en relación con los dispositivos conectados a la red.
- ✓ Se elimina la medida referida a medios alternativos.

PROTECCIÓN DE LAS COMUNICACIONES

- ✓ Experimentan un leve incremento de exigencia la protección de la confidencialidad, y la separación de flujos de información en la red.
- ✓ Se obliga a cifrar las redes privadas virtuales, cuando la comunicación discurra fuera del propio dominio de seguridad.
- ✓ Se aligera el perímetro seguro.
- ✓ Se eliminan los medios alternativos.

PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

- ✓ Se refuerzan levemente el borrado y destrucción.

PROTECCIÓN DE LAS APLICACINES INFORMÁTICAS

- ✓ Se incrementa significativamente la exigencia en aceptación y puesta en servicio, a la vista de los nuevos vectores de ataque propiciados por importantes vulnerabilidades en el software.

PROTECCIÓN DE LA INFORMACIÓN

- ✓ Se aligera calificación de la información.
- ✓ Se incrementa exigencia en datos de carácter personal y copias de seguridad.

PROTECCIÓN DE LOS SERVICIOS

- ✓ Se añade una nueva medida para la protección de la navegación web.
- ✓ Se aumenta la exigencia de protección frente a denegación de servicio.
- ✓ Se eliminan medios alternativos.

A la vista de lo recogido en los cuadros anteriores, en la propuesta incluida en este proyecto de nuevo RD del ENS se **fortalecen las medidas relativas a la identificación, la configuración de seguridad, la protección frente al código dañino, el registro de actividad, la gestión de capacidad, la detección de intrusiones, el sistema de métricas y la aceptación y puesta en servicio**.

También se refuerzan, aunque en menor medida, los requisitos de acceso, la gestión de cambios, la gestión de incidentes, el mantenimiento y las actualizaciones de seguridad, la protección de la confidencialidad y las copias de seguridad.

El resumen, una vez analizado por parte del CCN-CERT el histórico del informe INES y las lecciones aprendidas a lo largo de los últimos años en respuesta a los incidentes de seguridad, se han **reforzado las siguientes medidas**:

- ✓ Protección frente a código dañino [op.exp.6]
- ✓ Mecanismo con autenticación [op.acc.5] (no uso de doble factor)
- ✓ Detección de intrusión [op.mon.1]
- ✓ Copias de seguridad [mp.info.9]
- ✓ Perímetro seguro [mp.com.1]
- ✓ Segregación de redes [mp.com.4] (Redes NO segregadas)
- ✓ Configuración de seguridad [op.exp.2] y gestión de la configuración [op.exp.3]
- ✓ Mantenimiento [op.exp.4] (sistemas obsoletos, sin actualizaciones de seguridad)
- ✓ Concienciación [mp.per.3] y formación [mp.per.4]
- ✓ Protección de servicios y aplicaciones web [mp.s.2]

Por otra parte, se han añadido **nuevos controles**, como por ejemplo lo relativos a servicios en la nube, interconexión de sistemas, protección de la cadena de suministro (interpela a proveedores de TI de las Administraciones Públicas), medios alternativos, vigilancia y otros dispositivos conectados a la red.

Otras medidas, como segregación de tareas, sellos de tiempo, calificación de la información, protección de dispositivos portátiles, protección frente a denegación de servicio o perímetro seguro, se han **simplificado**, e incluso se **eliminan** algunas otras, como las relativas a personal alternativo, medios alternativos, al englobarse en controles diferentes.

En el siguiente cuadro se resumen las medidas eliminadas y las nuevas:

Medidas eliminadas	Nuevas medidas
✓ [op.acc.7] acceso remoto se ha incluido en [op.acc.4] protección de gestión de derechos de acceso. ✓ [op.exp.10] se ha recogido en [op.exp.8] protección de los registros de actividad. ✓ Las medidas que hacían referencia a medios, instalaciones y personal alternativo ([op.ext.9], [mp.if.9], [mp.per.9], [mp.eq.9], [mp.com.9], [mp.s.9]), se han aglutinado en la nueva medida ✓ [op.cont.4] medios alternativos. ✓ [mp.info.3] antigua medida de cifrado, se recoge ahora en otras medidas en las que se hace referencia expresa al cifrado de dispositivos portátiles, protección de la confidencialidad, criptografía y transporte ([mp.eq.3], [mp.com.2], [mp.si.2] y [mp.si.4] respectivamente).	✓ [op.ext.3] Protección de la cadena de suministro para categoría ALTA. ✓ [op.ext.4] Interconexión de sistemas desde categoría MEDIA. ✓ [op.nub] medidas para sistemas que suministran servicios en la nube a los organismos del sector público para todos los niveles y categorías. ✓ [op.cont.4] Medios alternativos. Para nivel ALTO. Aúna todas las referencias que se hacían a medios, instalaciones y personal alternativo. ✓ [op.mon.3] Vigilancia. Aplica a todas las categorías. ✓ [mp.eq.4] Otros dispositivos conectados a la red. Aplica a todas las categorías. ✓ [mp.s.3] Protección de la navegación web. Aplica a todas las categorías y se refuerza incluyendo la monitorización para categoría ALTA.

Ilustración 5 Panorámica de evolución de las medidas de seguridad. (Fuente: [11])

Si analizamos los cambios teniendo en cuenta la categoría, se observa que:

- Se incrementa el nivel de exigencia con relación a las medidas en el nivel BAJO, pasando de 45 controles a 53.
- Nivel MEDIO se incrementan ligeramente, prácticamente permanece igual.
- Nivel ALTO, se pasa de 75 a 73, después de un proceso de racionalización de los controles para esta categoría.

Ilustración 6 Evolución de los controles por categoría. (Fuente: [11])

Finalmente, en este proyecto de nuevo RD se han **codificado los requisitos de las medidas de protección** y para reconocer diferentes niveles de exigencia se emplean los denominados **refuerzos de seguridad**, también codificados, de manera que los controles se formulan según los requisitos base y los posibles refuerzos de seguridad (**R**), que se suman a los requisitos base de la medida.

3 Plan de Adecuación al ENS

Según se describe en la guía **CCN-STIC-806 Plan de Adecuación al ENS** [14], el plan de adecuación es el paso previo para abordar la posterior implantación del ENS y debe de desarrollarse mediante las siguientes actividades:

- Elaborar la **Política de Seguridad de la Información y la Normativa Interna correspondiente.**
- **Identificar los servicios** y **categorizar los sistemas de información**: valoración de servicios prestados e información tratada.
- Realizar el **Análisis de Riesgos.**
- Elaborar la **Declaración de Aplicabilidad**.
- Desarrollar un **Plan de mejora de la seguridad** en base al informe de insuficiencias detectadas.

Las características propias de las entidades locales más pequeñas, con recursos muy limitados, hacen difícil el cumplimiento del ENS de manera individualizada. Por este motivo desde el CCN y en colaboración con la FEMP se han impulsado inciativas con acciones concretas que contemplan mecanismos de adecuación enfocadas a abordar el proceso de adecuación y la posterior implantación del ENS a grupos de entidades locales homogéneos, mediante definición de un marco de certificación específico con el ENS (MCE-ENS) que facilite la consecución del objetivo final de certificación a este tipo de entidades [15].

Bajo este modelo se desarrolla la implantación conjunta del ENS en ayuntamientos de características tecnológicas y administrativas similares, contando con el del organismo superior (en nuestro caso la Diputación Provincial) del que dependen las entidades locales adheridas al MCE-ENS, con el objetivo de alcanzar la Certificación de Conformidad con el ENS para los sistemas de información que soporten los servicios municipales que se ofrezcan a través de Sede Electrónica.

Este modelo posibilita disponer de un marco normativo conjunto que permite a las EELL disponer de una **política de seguridad común** y un **Comité de Seguridad conjunto** para la dirección y el gobierno en materia de seguridad de la información.

El escenario propuesto en este TFM es tal que la Diputación Provincial, además de ser el organismo superior que define y dirige el MCE-ENS, es a su vez la entidad certificadora. El Plan de adecuación contempla tres fases, hasta legar al cumplimiento del ENS y la certificación del sistema de información de la entidad.

Ilustración 7 Fases del Plan de adecuación

Como se observa en la anterior imagen, se definen tres fases para nuestro proyecto de adecuación al ENS:

- "*current*": situación actual o punto de partida. En esta fase se aplican las medidas únicamente contenidas en el perfil de cumplimiento específico para entidades locales de menos de 5.000 habitantes detallado en la Tabla 16.
- "*intermediate*": fase intermedia durante la que se prioriza la implantación de las medidas más prioritarias, vinculadas al AR llevado a cabo en la fase anterior y a otros factores relacionados con negocio y el ámbito del MCE-ENS.
- "*final*": estado final de aplicación de las salvaguardas, que ha de coincidir con lo requerido por el ENS, en cualquier caso, puesto que su cumplimiento y la posterior certificación son los objetivos del Plan de Adecuación.

Más adelante, en los apartados 3.4 Análisis de riesgos y 3.5 Plan de mejora de la seguridad se detalla el proceso y sus fases.

3.1 Contexto del plan

Tal y como ya se adelantó en el apartado *Contexto y justificación del Trabajo*, el planteamiento elegido para este TFM es el de elaborar un Plan de adecuación al Esquema Nacional de Seguridad (ENS) para una **administración pública local**, toda vez que entre las entidades obligadas a adoptar el ENS están las que integran la Administración Local.

Se ha escogido como entidad objetivo un ayuntamiento ficticio de **menos de 5.000 habitantes** que ha de abordar la implantación y posterior certificación de cumplimiento del ENS en el contexto definido por un MCE-ENS impulsado por la Diputación Provincial correspondiente.

Los servicios que se encuentran dentro del alcance del ENS para una entidad local pueden identificarse con carácter general según lo indicado en la guía CCN-STIC-883 Guía de implantación del ENS para Entidades Locales [9]. Concretamente para el caso de nuestro ayuntamiento, en los documentos disponibles para su descarga relativos a *Ayuntamientos pequeños y con limitados recursos, de menos de 5.000 habitantes*, se relacionan las competencias municipales según el art. 25 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL) [16].

Al margen de que se puedan incluir dentro del alcance del ENS las competencias, servicios y activos de información indicados en la referencia anterior, como se explica más adelante se limitará dicho alcance a unos pocos servicios y activos de entre los que, con carácter general, podrían configurar una administración local del tipo de la elegida.

Se escogerá para ello principalmente los sistemas que ofrezcan servicios de Administración Electrónica al ciudadano, atendiendo a lo indicado en la página 29 de la *Guía estratégica en seguridad para entidades locales (Tomo I)* [17] publicada bajo el patrocinio de la FEMP, en donde, al hablar del ámbito de aplicación del ENS lo enfoca preferentemente a aquellos **medios electrónicos que faciliten directamente el ejercicio de derechos a los ciudadanos y a su relaciones con las Administraciones Públicas por dichos medios**.

Para la definición del escenario objeto de análisis, la entidad local elegida es un municipio costero atlántico, cuyas actividades económicas más relevantes son la pesca y la acuicultura, con un sector en desarrollo, pero con crecimiento sostenido, el turístico.

En un ayuntamiento de estas características, las áreas municipales más comunes podrían ser las siguientes:

- Urbanismo, Economía, Hacienda, y Servicios Sociales
- Turismo, Cultura y Deportes
- Servicios, Tráfico, Trabajo y Mar
- Medio Ambiente y Participación Ciudadana
- Obras, Educación y Personal
- Familia, Mujer y Juventud

La entidad dispone de una **página web municipal** de carácter oficial en la que fundamentalmente se publica información descriptiva acerca del municipio, la estructura administrativa y de gobierno del ayuntamiento y sus servicios. Desde este portal se puede acceder a la **Sede Electrónica** de su titularidad. Tanto el portal web como la Sede Electrónica están externalizados en su totalidad, tanto el software como la infraestructura que da soporte al sistema, incluyendo el Sistema Gestor de Bases de Datos (SGBD).

También está externalizado el **servicio de tramitación**, mediante la externalización de la aplicación de gestión correspondiente y la infraestructura que soporta dicho servicio y lo publica en internet, al tratarse de un servicio web.

Además de información de carácter generalista sobre el municipio, en el portal web municipal se incluyen los siguientes servicios:

- Objetos perdidos – Policía local (Nombre, email, tfno.)
- Noticias
- Tablón de anuncios
- Descarga de formularios (.pdf) para diferentes trámites
- Contacto (Nombre, email)

Edificios Municipales:

- Ayuntamiento (alberga las oficinas centrales y el CPD)
- Consultorio médico
- Policía Local

- Auditorio Municipal
- Centro de interpretación del medio marino
- Biblioteca municipal
- Punto Limpio

Servicios externos:

- Portal web y sede electrónica (aplicaciones e infraestructura).
- Sistema de Tramitación de expedientes (aplicaciones e infraestructura).
- Perfil del Contratante (Plataforma de la Comunidad Autónoma).
- Servicio de asistencia técnica de TI.
- Conexión a Internet (operador de telecomunicaciones)

Esto dibuja un escenario para el análisis que pretende recrear condiciones asimiladas a una situación real de una entidad local de menos de 5.000 habitantes.

3.1.1 Identificación de los Servicios y la Información que manejan

SERVICIO: Registro municipal de entrada/salida

Su función es la recepción de solicitudes, escritos y comunicaciones órgano municipal, así como la expedición de recibos de la presentación de dichas solicitudes, escritos y comunicaciones.

Se ha integrado un **Registro Electrónico** que tiene como finalidad la recepción, digitalización y remisión de documentación en formato electrónico, remitida por personas físicas o jurídicas, órganos o unidades administrativas identificadas y autenticadas de acuerdo con los criterios de certificación y firma electrónica que marca la legislación vigente.

Información almacenada. Dada su propia naturaleza, la información contenida es de un perfil altamente heterogéneo, relacionada con cualquiera de las áreas municipales y sus procesos de negocio. En general, entre otras:

- Datos identificativos de ciudadanos y entidades
- Datos de proveedores
- Datos de personal
- Datos relativos a los expedientes de diferente naturaleza
- Datos económicos

SERVICIO: Tramitación de Expedientes

Su objetivo es proveer soporte a la gestión municipal de todos los expedientes administrativos propios de una entidad local de estas características, es decir, que estén en su ámbito competencial.

Este servicio es utilizado por el personal de las diferentes áreas municipales para la tramitación de los expedientes y el control presupuestario y del gasto, así como por los miembros del gobierno para la consulta de la situación de dichos expedientes y la elaboración de informes de gestión y estadísticas.

Información almacenada:

- Datos identificativos de ciudadanos y entidades
- Datos de proveedores

- Datos de personal
- Datos relativos a los expedientes de diferente naturaleza
- Datos económicos

SERVICIO: Portal web

Página web oficial del ayuntamiento, de carácter fundamentalmente informativo, donde se publica información general de interés público sobre el ayuntamiento, para ser consultada tanto por el ciudadano del propio ayuntamiento como por el visitante o cualquier persona interesada en el conocimiento del municipio.

Información almacenada:

- Objetos perdidos
- Información descriptiva sobre la administración municipal (estructura, órganos de gobierno, información de contacto, etc.)
- Información sobre el municipio (población, economía, patrimonio, turismo, etc.)
- Tablón de anuncios
- Noticias municipales

SERVICIO: Sede Electrónica

Dirección electrónica disponible para los ciudadanos a través de internet y cuya titularidad corresponde al ayuntamiento.

A través de este servicio se posibilita el acceso del ciudadano para la realización de todas las actuaciones, trámites y procedimientos en relación a la municipalidad, según la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL) [16]. Constituye, por tanto, el principal punto de acceso del ciudadano a los servicios de Administración Electrónica.

Información almacenada:

- Datos identificativos de ciudadanos y entidades
- Datos relativos a los asuntos de diferente naturaleza que pueden ser objeto de solicitud o comunicación a través de la Sede.
- Datos económicos
- Datos de proveedores
- Datos de personal
- Datos relativos a los expedientes de diferente naturaleza

3.1.2 Sistemas de información

Partiendo de las relaciones funcionales entre los diferentes servicios identificados, y agrupándolos de manera lógica según su nivel de integración, se identifican los siguientes sistemas:

- **Sistema de gestión municipal (SGM)**: Agrupa todos los servicios relacionados con la tramitación de los expedientes municipales de las diversas áreas de gobierno y la gestión de los recursos del órgano (tramitación, gestión económica y presupuestaria, RRHH, etc.). En sí mismo constituye el *core* de la gestión y administración municipal y puede entenderse como el *backend* para la denominada Administración Electrónica.

Funciones que ofrece

- Tramitación de expedientes de diferentes áreas municipales (urbanismo, servicios, obras, etc.).
- Gestión presupuestaria y económica.
- Gestión de proveedores y contratos.
- Gestión de RRHH

- **Sistema de Administración Electrónica (AE)**: Agrupa todos los servicios que se prestan por medio de la sede electrónica del órgano municipal en el ejercicio de sus competencias.

Funciones que ofrece

- Carpeta Electrónica (notificaciones, consulta expedientes, registros presentados, datos)
- Buzón electrónico
- Quejas y sugerencias
- Portafirmas
- Factura electrónica
- Presentación de instancias genéricas
- Validación de documentos
- Trámites, entre otros, figuran los siguientes:
  - Solicitudes de diversas certificaciones
  - Padrón municipal (Altas/Bajas/Modificaciones)
  - Matrimonio civil
  - Registro parejas de hecho
  - Presentación de documentos
  - Presentación solicitudes relacionadas con obras, urbanismo, vivienda y actividades económicas
  - Solicitudes de del personal del ayuntamiento
  - Interposición de recursos
  - Ejercicio de los Derechos de Rectificación, Supresión, Limitación, Portabilidad u Oposición en relación con Datos de Carácter Personal
  - Ejercicio do Derecho de Acceso (Datos de Carácter Personal)
  - Solicitud de contacto con personal municipal
  - Solicitud de Licencia de Actividades y Espectáculos Públicos

En el siguiente cuadro se sintetiza la asociación de los servicios con los sistemas identificados:

SISTEMA	SERVICIO
SISTEMA DE GESTIÓN MUNICIPAL (SGM)	Registro municipal de entrada/salida
	Tramitación de Expedientes
SISTEMA DE ADMINISTRACIÓN ELECTRÓNICA (AE)	Portal web
	Servicio de Sede Electrónica

Tabla 3 Sistemas y Servicios de la entidad local objetivo.

3.2 Categorización del Sistema

La valoración y catalogación de los sistemas es uno de los elementos fundamentales del ENS, puesto que a partir de él se determinan los controles de seguridad que será necesario aplicar.

Para la determinación de los niveles y categorías se analizan los elementos esenciales de información y servicios apoyándose de manera general en lo descrito en el Anexo I del ENS y en la guía *CCN-STIC 803 Valoración de los sistemas* [8].

Se resumen a continuación los criterios generales seguidos para la valoración de la Información y los Servicios:

DIMENSIÓN	Criterios generales de valoración de Información	Criterios generales de valoración de Servicios
Confidencialidad [C]	El nivel de seguridad requerido para la Confidencialidad se establece en función de las consecuencias que tendría la revelación a personas no autorizadas o que no necesitan conocer la información.	
Integridad [I]	El nivel de seguridad requerido para la Integridad se establece en función de las consecuencias que tendría la modificación de la información por parte de alguien que no está autorizado.	Los requisitos de Integridad sobre un servicio derivan de la información que maneja. Incluye la posibilidad de que la información quede en estado impropio porque el servicio no se complete adecuadamente.
Autenticidad [A]	El nivel de seguridad requerido para la Autenticidad se establece en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.	El nivel de seguridad requerido para la Autenticidad se establece en función de las consecuencias que tendría el hecho de el servicio fuera usado por personas indebidamente autenticadas.
Trazabilidad [T]	El nivel de seguridad requerido para la Trazabilidad se establece en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido y/o modificado la información.	El nivel de seguridad requerido para la Trazabilidad se establece en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.
Disponibilidad [D]	El nivel de seguridad requerido para la Disponibilidad se establece en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.	El nivel de seguridad requerido para la Disponibilidad se establece en función de las consecuencias que tendría el que una persona autorizada no pudiera usar el servicio cuando lo necesita.

Tabla 4 Criterios generales de valoración de la Información y los Servicios.

Para el caso concreto de las Entidades Locales de menos de 5.000 habitantes, incluido bajo el epígrafe de la guía *CCN-STIC 883* [9], el CCN ha publicado también el *Anexo I. Plan Adecuación Ayuntamientos - 20.000* y *CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (menos de 5.000 habitantes)* en la que se realiza una **propuesta de valoración de los diferentes Servicios e Información** identificados de manera global y estandarizada para una administración municipal.

En base a ello, la categorización propuesta con carácter general para el sistema de ayuntamientos de menos de 20.000 habitantes es de nivel MEDIO:

SISTEMA DE INFORMACIÓN DEL AYUNTAMIENTO					
NIVELES MÁXIMOS	[C]	[I]	[D]	[A]	[T]
NIVEL MÁXIMO DE LOS SERVICIOS	[M]	[M]	[M]	[M]	[M]
NIVEL MÁXIMO DE LA INFORMACIÓN	[M]	[M]	[M]	[M]	[M]
NIVELES MÁXIMOS	**[M]**	**[M]**	**[M]**	**[M]**	**[M]**
CATEGORÍA MEDIA [C=M, I =M, D=M, A=M, T=M]					

Ilustración 8 Modelo de valoración de las dimensiones del sistema (Fuente: CCN-STIC 883 - Anexo I. Plan Adecuación Ayuntamientos - 20.000)

A continuación, se detalla la valoración efectuada para cada uno de los Sistemas y Servicios identificados objeto de análisis.

3.2.1 Sistema de Gestión Municipal (SGM) – Servicio de Registro municipal de entrada/salida

Valoración de la Información

Dimensión	Nivel	Motivo
Confidencialidad [C]	Medio	Perjuicio grave. Autorización explícita de acceso.
Integridad [I]	Medio	Perjuicio grave. Incumplimiento legal
Autenticidad [A]	Medio	Perjuicio grave. Autenticidad de documento electrónico.
Trazabilidad [T]	Medio	Perjuicio grave. Sellado de tiempo en documentos electrónicos.
Disponibilidad [D]	n/a	Se valora en el servicio

Tabla 5 Valoración Información SGM-Registro.

Valoración del Servicio

Dimensión	Nivel	Motivo
Confidencialidad [C]	n/a	Se valora en la Información
Integridad [I]	n/a	Se valora en la Información
Autenticidad [A]	n/a	Se valora en la Información
Trazabilidad [T]	n/a	Se valora en la Información
Disponibilidad [D]	Bajo	Perjuicio limitado. Puede ser fácilmente reparable.

Tabla 6 Valoración servicio SGM-Registro.

3.2.2 Sistema de Gestión Municipal (SGM) – Tramitación de Expedientes

Valoración de la Información

Dimensión	Nivel	Motivo
Confidencialidad [C]	Medio	Perjuicio grave. Información relacionada con la gestión de RRHH, información económica y datos personales asociados a condiciones de minusvalías, etc.
Integridad [I]	Medio	Perjuicio grave. Incumplimiento legal y daño económico relevante para el órgano.
Autenticidad [A]	Medio	Perjuicio grave. Equiparable a la Integridad.
Trazabilidad [T]	Bajo	Perjuicio limitado. Dificultaría el seguimiento y corrección de errores.
Disponibilidad [D]	n/a	Se valora en el servicio

Tabla 7 Valoración Información SGM-Tramitación.

Valoración del Servicio

Dimensión	Nivel	Motivo
Confidencialidad [C]	n/a	Se valora en la Información
Integridad [I]	n/a	Se valora en la Información
Autenticidad [A]	n/a	Se valora en la Información
Trazabilidad [T]	n/a	Se valora en la Información
Disponibilidad [D]	Bajo	Perjuicio limitado. Puede ser subsanable sin perjuicio mayor.

Tabla 8 Valoración Servicio SGM-Tramitación.

3.2.3 Sistema de Administración Electrónica (AE) – Portal web

Valoración de la Información

Dimensión	Nivel	Motivo
Confidencialidad [C]	Bajo	Perjuicio limitado. No contiene información muy relevante para esta dimensión.
Integridad [I]	Medio	Perjuicio grave. Pérdida de reputación y protestas ciudadanas.
Autenticidad [A]	Bajo	Perjuicio limitado.
Trazabilidad [T]	Bajo	Perjuicio limitado.
Disponibilidad [D]	n/a	Se valora en el servicio.

Tabla 9 Valoración Información AE-Portal.

Valoración del Servicio

Dimensión	Nivel	Motivo
Confidencialidad [C]	n/a	Se valora en la Información
Integridad [I]	n/a	Se valora en la Información
Autenticidad [A]	n/a	Se valora en la Información
Trazabilidad [T]	n/a	Se valora en la Información
Disponibilidad [D]	Bajo	Perjuicio limitado. Pérdida poco relevante de reputación y escaso impacto en la ciudadanía.

Tabla 10 Valoración Servicio AE-Portal.

3.2.4 Sistema de Administración Electrónica (AE) – Servicio de Sede Electrónica

Valoración de la Información

Dimensión	Nivel	Motivo
Confidencialidad [C]	Medio	Portal web donde se relacionan y enlazan los servicios de Administración Electrónica.
Integridad [I]	Medio	Perjuicio grave. Incumplimiento legal por modificación de la información.
Autenticidad [A]	Medio	Perjuicio grave. Ataques de suplantación
Trazabilidad [T]	Bajo	Perjuicio limitado. Errores fácilmente reparables.
Disponibilidad [D]	n/a	Se valora en el servicio.

Tabla 11 Valoración Información AE-Sede.

Valoración del Servicio

Dimensión	Nivel	Motivo
Confidencialidad [C]	n/a	Se valora en la Información
Integridad [I]	n/a	Se valora en la Información
Autenticidad [A]	n/a	Se valora en la Información
Trazabilidad [T]	n/a	Se valora en la Información
Disponibilidad [D]	Medio	Perjuicio grave. En función de la pérdida reputacional significativa y la demanda del servicio por parte de la ciudadanía, puede considerarse aceptable hasta 1d de RTO.

Tabla 12 Valoración Servicio AE-Sede.

3.2.5 Categorización global del Sistema de Información

El resultado de la valoración realizada sobre los servicios y la información en los apartados anteriores se resume en la siguiente tabla:

Servicio	Confidencialidad [C]	Integridad [I]	Autenticidad [A]	Trazabilidad [T]	Disponibilidad [D]	Nivel Global
SGM Registro municipal de entrada/salida	Medio	Medio	Medio	Medio	Bajo	**Medio**
SGM Tramitación de Expedientes	Medio	Medio	Medio	Bajo	Bajo	**Medio**
AE Portal web	Bajo	Medio	Bajo	Bajo	Bajo	**Medio**
AE Servicio de Sede Electrónica	Medio	Medio	Medio	Bajo	Medio	**Medio**

Tabla 13 Categoría de los servicios.

En consecuencia, y siguiendo las indicaciones para la categorización indicadas en el Anexo I del ENS, así como las recomendaciones de las guías CCN-STIC 803 y CCN-STIC 883, la categorización de los sistemas es la siguiente:

Sistema	Confidencialidad [C]	Integridad [I]	Autenticidad [A]	Trazabilidad [T]	Disponibilidad [D]	Nivel Global
SISTEMA DE GESTIÓN MUNICIPAL (SGM)	Medio	Medio	Medio	Medio	Bajo	**Medio**
SISTEMA DE ADMINISTRACIÓN ELECTRÓNICA (AE)	Medio	Medio	Medio	Bajo	Medio	**Medio**

Tabla 14 Categoría global de los sistemas.

3.3 Selección de las medidas de seguridad

Una vez categorizados los sistemas de información, es necesario determinar los controles de seguridad que serán de aplicación a los sistemas objeto del Plan de Adecuación al ENS y que posteriormente se recogerán en la **Declaración de Aplicabilidad**

En este documento se utiliza la codificación definida en el ENS para las diferentes familias de medidas de seguridad:

Código	Significado
org	**Marco organizativo**
op	**Marco operacional**
op.pl	Marco operacional. Planificación
op.acc	Marco operacional. Control de acceso
op.exp	Marco operacional. Explotación
op.ext	Marco operacional. Servicios externos
op.cont	Marco operacional. Continuidad del servicio
op.mon	Marco operacional. Monitorización del sistema
mp	**Medidas de protección**
mp.if	Medidas de protección. Protección de las instalaciones e infraestructuras
mp.per	Medidas de protección. Gestión del personal
mp.eq	Medidas de protección. Protección de los equipos
mp.com	Medidas de protección. Protección de las comunicaciones
mp.si	Medidas de protección. Protección de los soportes de información
mp.sw	Medidas de protección. Protección de las aplicaciones informáticas
mp.info	Medidas de protección. Protección de la información
mp.s	Medidas de protección. Protección de los servicios

Tabla 15 Nomenclatura para los controles ENS.

Para facilitar la conformidad con el ENS a tipos de entidades concretos, el CCN-CERT formula la implementación de perfiles de cumplimiento específicos que, atendiendo al principio general de proporcionalidad, incluyen un conjunto de controles que se adecúen a una categoría de seguridad concreta y que conformen el preceptivo análisis de riesgos del sistema de información de dichas entidades.

Un **perfil de cumplimiento específico** es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 3/2010, de 8 de enero, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Fuente: CCN-STIC 883A – Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos.

Este perfil permitirá la implantación del ENS en una primera fase aplicando una serie de medidas como si el sistema presentara necesidades de seguridad de categoría básica, para lo cual en nuestro caso basta una simple autoevaluación realizada por parte del personal puesto a disposición por el organismo superior en el ámbito del MCE-ENS. En una segunda y tercera fases, se abordaría la implantación de las medidas necesarias para el cumplimiento en categoría MEDIA.

Según el perfil de cumplimiento específico definido por el CCN-CERT para los ayuntamientos pequeños de menos de 5.000 habitantes con limitados recursos [7] se ha determinado que las medidas que son de aplicación y el nivel de seguridad de cada una de ellas son las que se indican en la siguiente tabla:

Dimensiones					
Afectadas	CAT B	CAT M	CAT A		
				Control	Aplicación
categoría	aplica	=	=	[org.1]	BAJO*
categoría	aplica	=	=	[org.2]	BAJO*
categoría	aplica	=	=	[org.3]	BAJO*
categoría	aplica	=	=	[org.4]	BAJO
categoría	aplica	+	++	[op.pl.1]	BAJO*
categoría	aplica	+	++	[op.pl.2]	BAJO
categoría	aplica	=	=	[op.pl.3]	BAJO
D	n.a.	aplica	=	[op.pl.4]	n/a[1]
Todas	n.a.	aplica	aplica	[op.pl.5]	n/a
A T	aplica	=	=	[op.acc.1]	BAJO
I C A T	aplica	=	=	[op.acc.2]	BAJO
I C A T	n.a.	aplica	=	[op.acc.3]	n/a
I C A T	aplica	=	=	[op.acc.4]	BAJO
I C A T	aplica	+	++	[op.acc.5]	BAJO
I C A T	aplica	+	++	[op.acc.6]	BAJO

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación
I C A T	aplica	+	=	[op.acc.7]	MEDIO
Todas	aplica	=	=	[op.exp.1]	BAJO*
Todas	aplica	=	=	[op.exp.2]	BAJO*
Todas	n.a.	aplica	=BAJO	[op.exp.3]	n/a
Todas	aplica	=	=	[op.exp.4]	BAJO
Todas	n.a.	aplica	=	[op.exp.5]	n/a
Todas	aplica	=	=	[op.exp.6]	BAJO
Todas	n.a.	aplica	=	[op.exp.7]	MEDIO*
T	aplica	+	++	[op.exp.8]	BAJO*
Todas	n.a.	aplica	=	[op.exp.9]	MEDIO*
T	n.a.	n.a.	Aplica	[op.exp.10]	n/a
Todas	aplica	+	=	[op.exp.11]	BAJO
Todas	n.a.	aplica	=	[op.ext.1]	MEDIO*
Todas	n.a.	aplica	=	[op.ext.2]	MEDIO*
D	n.a.	aplica	=	[op.ext.9]	n/a
D	n.a.	aplica	=	[op.cont.1]	n/a
D	n.a.	n.a.	aplica	[op.cont.2]	n/a
D	n.a.	n.a.	aplica	[op.cont.3]	n/a
Todas	aplica	aplica	=	[op.mon.1]	n/a
Todas	aplica	+	++	[op.mon.2]	MEDIO*
Todas	aplica	=	=	[mp.if.1]	BAJO
Todas	aplica	=	=	[mp.if.2]	BAJO
Todas	aplica	=	=	[mp.if.3]	BAJO
D	aplica	+	=	[mp.if.4]	BAJO
D	aplica	=	=	[mp.if.5]	BAJO
D	n.a.	aplica	=	[mp.if.6]	n/a
Todas	aplica	=	=	[mp.if.7]	BAJO

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación
D	n.a.	n.a.	aplica	[mp.if.9]	n/a
Todas	n.a.	aplica	=	[mp.per.1]	n/a
Todas	aplica	=	=	[mp.per.2]	BAJO
Todas	aplica	=	=	[mp.per.3]	BAJO
Todas	aplica	=	=	[mp.per.4]	BAJO
Todas	n.a.	n.a.	aplica	[mp.per.9]	n/a
Todas	aplica	+	=	[mp.eq.1]	BAJO
A	n.a.	aplica	+	[mp.eq.2]	n/a
Todas	aplica	=	+	[mp.eq.3]	BAJO
D	n.a.	n.a.	aplica	[mp.eq.9]	n/a
Todas	aplica	=	+	[mp.com.1]	BAJO
C	n.a.	aplica	+	[mp.com.2]	MEDIO*
I A	aplica	+	++	[mp.com.3]	MEDIO*
Todas	n.a.	n.a.	aplica	[mp.com.4]	n/a
D	n.a.	n.a.	aplica	[mp.com.9]	n/a
C	aplica	=	=	[mp.si.1]	BAJO*
I C	n.a.	aplica	=	[mp.si.2]	n/a*
categoría	aplica	=	=	[mp.si.3]	BAJO*
categoría	aplica	=	=	[mp.si.4]	BAJO*
C	aplica	+	=	[mp.si.5]	BAJO*
categoría	n.a.	aplica	=	[mp.sw.1]	n/a
categoría	aplica	+	++	[mp.sw.2]	n/a*
categoría	aplica	=	=	[mp.info.1]	BAJO
C	aplica	+	=	[mp.info.2]	BAJO
C	aplica	=	=	[mp.info.3]	n/a
I A	aplica	+	++	[mp.info.4]	*
T	n.a.	n.a.	aplica	[mp.info.5]	ALTO*

Dimensiones					
Afectadas	CAT B	CAT M	CAT A		
				Control	Aplicación
C	aplica	=	=	[mp.info.6]	BAJO
D	aplica	=	=	[mp.info.9]	n/a*
Todas	aplica	=	=	[mp.s.1]	BAJO
Todas	aplica	=	+	[mp.s.2]	n/a*
D	n.a.	aplica	+	[mp.s.8]	n/a
D	n.a.	n.a.	aplica	[mp.s.9]	n/a

Tabla 16 Perfil de cumplimiento especifico para ayuntamientos pequeños.

En la tabla anterior, la columna "***Afectadas***" indica que una medida protege específicamente una cierta dimensión de seguridad, explicitada por su inicial: Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C], Trazabilidad [T].

Las columnas "***CAT B***", "***CAT M***" y "***CAT A***" recogen los niveles de seguridad exigidos en cada una de las dimensiones para cada medida o control.

En la columna "***Control***" se indica la medida de seguridad según la nomenclatura detallada en la tabla Tabla 15.

n.a.; Control de seguridad no aplicable.

aplica; Control de seguridad aplicable para las dimensiones o categoría indicados.

El signo "**=**" indica que las exigencias de un nivel son iguales a los del nivel inferior.

Los signos "**+**" y "**++**" indican el incremento de exigencias graduado en función del nivel de la dimensión de seguridad.

El "*****" indica que disponen de criterios específicos de aplicación, los cuales se detallan en el apartado 7.1 ANEXO I CRITERIOS DE APLICACIÓN DE MEDIDAS de este documento de TFM

De las 75 medidas de seguridad definidas en el Anexo II del ENS, se aplican en este perfil de cumplimiento específico un total de 48, y por tanto serán estas las que constituyan el objetivo de medidas a aplicar en la primera fase del plan de adecuación.

3.4 Análisis de riesgos

En el contexto de este TFM, restringimos el caso de aplicación únicamente al sistema denominado SISTEMA DE ADMINISTRACIÓN ELECTRÓNICA (AE), es decir, se selecciona aquel sistema que ofrece servicios directamente al ciudadano, siguiendo lo indicado en el apartado *3.1 Contexto del plan* de este documento.

Por otra parte, se centra el análisis únicamente en las dimensiones contempladas por el RD 3/2010 del ENS, es decir: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad. Se descartan, por tanto, otras dimensiones

relacionadas con la protección de datos de carácter personal, que quedan fuera del alcance de este trabajo.

Para el desarrollo del análisis de riesgos se ha escogido la metodología MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [18].

Esta metodología implementa el proceso de la gestión de riesgos dentro de un marco de trabajo de gobernanza como el definido por el estándar internacional ISO 31000 para la gestión de los riesgos en las organizaciones. De este modo, MAGERIT da soporte a la toma informada de decisiones en cuanto a los riesgos derivados del uso de las TI.

Según se recoge en el Art. 13.2 del RD 3/2010, para el análisis de riesgos se ha de emplear alguna metodología reconocida internacionalmente. MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de la *European Union Agency for Cybersecurity* (ENISA) [19].

La aplicación PILAR [20] es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de uso generalizado no solo por las Administraciones Públicas en España, sino también por las de otros países.

Para el desarrollo del Análisis de Riesgos (AR) en este TFM, se ha utilizado la versión PILAR RM (2021.1.10 – 5.11.2021), que permite analizar los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para el tratamiento de los riesgos la aplicación ofrece salvaguardas, normas y procedimientos de seguridad, analizándose el riesgo residual a lo largo de diversas etapas de tratamiento.

Esta herramienta permite hacer uso de una serie de bibliotecas para el tratamiento de los riesgos. En nuestro caso en concreto se han seleccionado las siguientes:

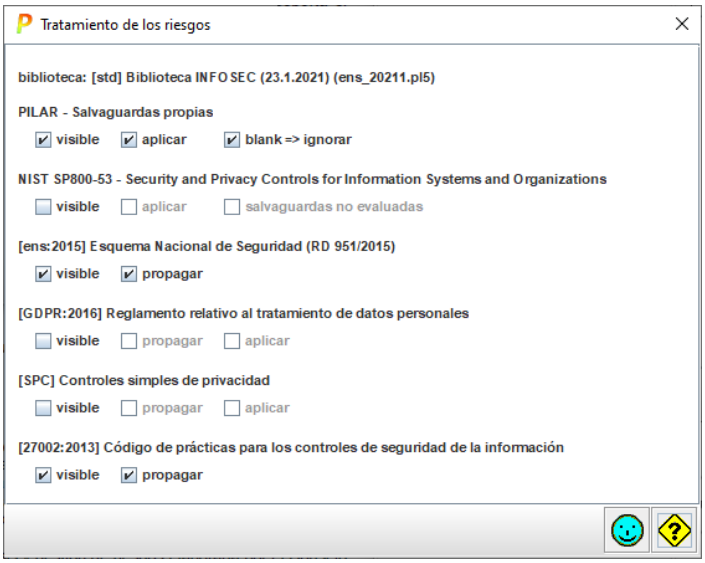


Ilustración 9 Bibliotecas empleadas en PILAR para el tratamiento de Riesgos.

En cuanto a la metodología empleada, MAGERIT, elaborada por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración

Electrónica, del Ministerio de Hacienda y Administraciones Públicas, permite abordar de una manera sistemática los procesos de análisis y tratamiento de riesgos, que posteriormente puedan dar lugar a un plan de gestión de la seguridad alineado con los objetivos estratégicos definidos por la organización.

El análisis de riesgos tiene en consideración los **activos** de la organización que componen su sistema de información, las **amenazas** sobre ellos que pueden acusar un perjuicio y las **salvaguardas** o medidas de protección para hacer frente a dichas amenazas. Analizando estos elementos se lleva a cabo una estimación del posible **impacto** y el **riesgo** de que se materialice, para finalmente trazar una estrategia de tratamiento de esos riesgos. En definitiva, el análisis de riesgos es una aproximación metodológica al problema de identificar qué necesidades tiene la organización en materia de seguridad, una vez identificadas las vulnerabilidades del sistema y las amenazas a las que está expuesto.

> El **riesgo** es una combinación entre la probabilidad de que una amenaza se materialice y el impacto que tendría si finalmente se produce, de forma que será mayor cuanta más probabilidad de ocurrencia de la amenaza y cuanto mayor impacto sobre el negocio.

Para realizar el análisis de riesgos se han de seguir metódicamente una serie de pasos:

1. Determinar los activos relevantes, las dependencias entre ellos y su valoración.
2. Determinar las amenazas a las cuales están expuestos
3. Identificar las salvaguardas disponibles y su eficacia frente al riesgo
4. Estimar el impacto en caso de que las amenazas se materialicen
5. Estimar el riesgo en función del impacto y la probabilidad de que se materialice la amenaza.

La siguiente ilustración es una abstracción del proceso:

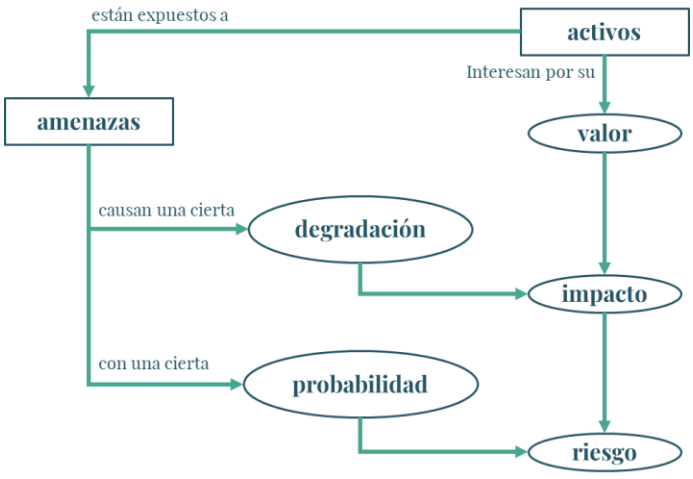


Ilustración 10 Elementos del análisis de riesgos.

Dicho lo anterior, de manera natural se puede concluir que la gestión de riesgos ha de planificar de antemano la respuesta a cada riesgo en caso de que este se materialice, para lo cual se establecerán controles que actúen sobre alguno de los dos factores que potencian el riesgo. Es decir, esos controles irán enfocados, bien a disminuir la

probabilidad de que una amenaza se materialice (Preventivos), o bien a reducir el impacto de la misma (Correctivos).

Antes de proseguir con el análisis de riesgos, definamos algunos conceptos en el contexto de la metodología MAGERIT [18] que es oportuno recordar:

- **Activo**: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Entre ellos, dentro de un sistema de información hay dos esenciales: la **información** que maneja y los **servicios** que presta. Estos activos esenciales marcan los requisitos de seguridad para todos los demás elementos que componen el sistema.
- **Dependencias** (entre activos): Los activos esenciales indicados en el punto anterior dependen de otros, como, por ejemplo, los equipos, las comunicaciones e incluso las personas. Las dependencias de alguna manera son la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior. Tal y como se indica en la guía CCN-STIC 470 PILAR – Manuela de usuario v7.1 [21], las dependencias proporcionan una transferencia controlada de valor. Como reglas generales:
  - la información esencial depende de los servicios esenciales
  - los servicios esenciales dependen del equipamiento (hw, sw, comunicaciones y soportes de información)
  - los equipos materiales dependen de las instalaciones
  - todos los activos dependen de los usuarios que puede dañarlos con sus actividades

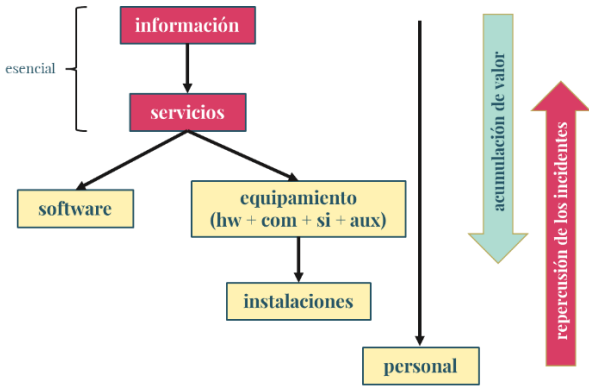


Ilustración 11 Reglas para árboles de dependencias.

  Un activo superior depende de otro inferior cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. Una amenaza que se materialice sobre un activo inferior, repercute en el activo superior.

- **Valor**: Cuanto mayor valor posee un activo, mayor nivel de protección necesitará. El valor puede ser **propio** o **acumulado**. En el esquema de dependencias de la Ilustración 11 la flecha vertical verde indica la acumulación de valor. Los activos inferiores acumulan el valor de los activos que se apoyan en ellos.

  El valor nuclear es el del activo esencial o de más alto nivel. En nuestro esquema, la **información** y los **servicios**. De esta manera, al valorar los activos superiores, los que son importantes por si mismos, de forma automática ese valor se acumula en los activos inferiores, añadiéndose a su valor propio.

La valoración puede ser cuantitativa (numérica absoluta) y cualitativa (escala de niveles). En nuestro caso utilizaremos una **valoración cualitativa**, lo que nos permitirá agilizar la valoración de los activos.

- **Amenazas**: Son la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Pueden variar de un activo a otro y también según la dimensión de seguridad que se considere, pues no todas las dimensiones se ven afectadas por todas las amenazas.
- **Impacto**: es la medida del daño sufrido por un activo debido a que se ha materializado una amenaza. Cuando se calcula sobre el valor acumulado del activo se denomina **impacto acumulado**. Este cálculo se efectúa para cada activo, amenaza y dimensión de seguridad, y es tanto mayor cuanto mayor son el valor acumulado del activo y la degradación sufrida.

  Cuando el impacto se calcula teniendo en consideración el valor propio del activo, se denomina **impacto repercutido**. Además de ser proporcional al valor del activo y a la degradación sufrida, será tanto mayor cuanto mayor sea la dependencia del activo.
- **Riesgo**: como ya adelantamos anteriormente, riesgo es la medida del daño probable sobre un sistema. Se deriva, pues, del impacto de las amenazas sobre los activos y de la probabilidad de ocurrencia. Por lo tanto, el riesgo aumenta con el impacto y con la probabilidad. Cuando para determinar el nivel de riesgo se utiliza el impacto cumulado, se denomina **riesgo acumulado** (es el que se calcula sobre los activos que soportan el peso del sistema de información y por lo tanto permite definir las salvaguardas sobre los medios de trabajo), y si se emplea el impacto repercutido se denomina **riesgo repercutido** (al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias sobre el sistema de información).

  Los riesgos potenciales se tratan adoptando medidas (salvaguardas) que los reducen. El nivel de riesgo que permanece después de haber implantado dichas medidas se denomina **riesgo residual**.
- **Salvaguarda**: procedimiento, herramienta o mecanismo tecnológico que reduce el riesgo, bien disminuyendo el impacto o la probabilidad (salvaguarda preventiva). Las salvaguardas se seleccionarán en función del tipo de activo, la dimensión que requiere protección, las amenazas de las que pretendemos protegernos y si existen o no otras salvaguardas alternativas.

  A la hora de determinar las salvaguardadas a aplicar en un sistema de información, es relevante tener en consideración el **principio de proporcionalidad**, es decir, el coste de la protección no debe ser superior al valor del bien protegido ni aplicarse ante amenazas que no vayan a suceder. En función de esto, puede darse la circunstancia de que una salvaguarda **no aplique**, simplemente porque no protege frente a la amenaza considerada, o que **no se justifica**, puesto que es desproporcionada frente al riesgo que se pretende proteger.

La relación de las salvaguardas o medidas seleccionadas para proteger un determinado sistema de información constituirá la denominada "**declaración de aplicabilidad**".

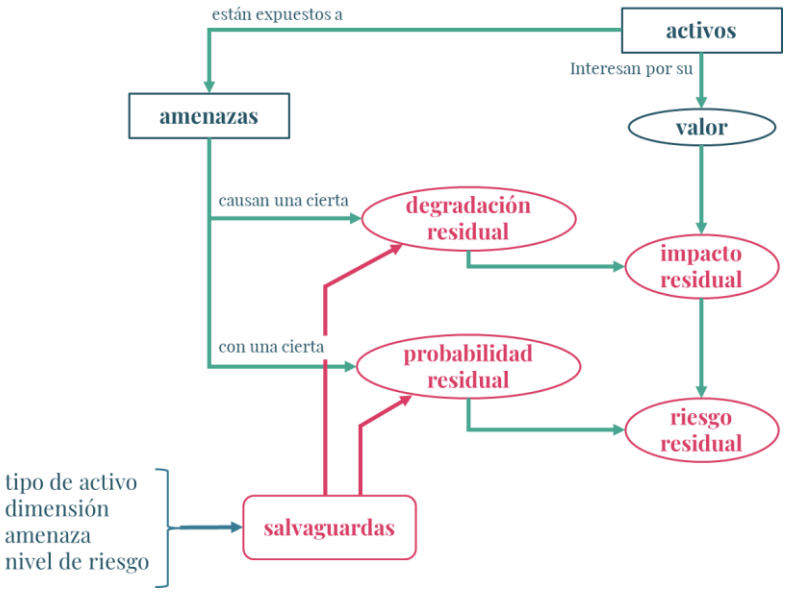


Ilustración 12 Elementos de análisis del riesgo residual.

- **Impacto residual**: es el impacto que permanece en el sistema después de haber implantado las salvaguardas definidas.

3.4.1 Escenario del análisis

En la siguiente ilustración se muestra a alto nivel la arquitectura lógica de red del escenario que debemos modelar para el análisis de riesgos.

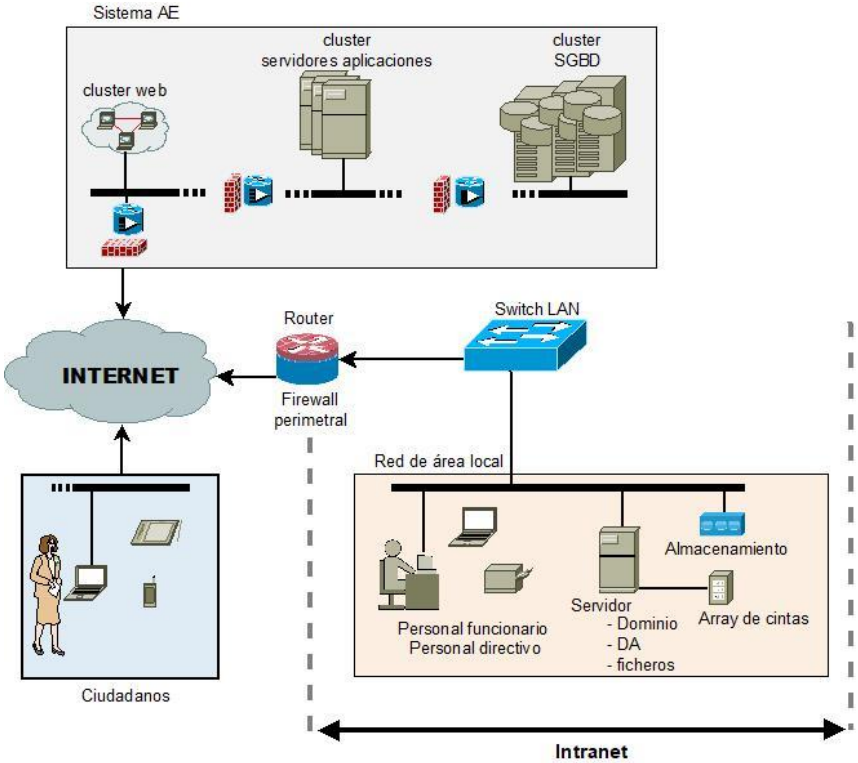


Ilustración 13 Arquitectura lógica de red.

En el diagrama de la Ilustración 13 se distinguen las siguientes áreas:

- **Intranet**:

  Es la red interna de la organización. En un único segmento de red se ubican los puestos de trabajo del personal funcionario, los portátiles del personal directivo de las áreas del gobierno local, impresoras multifunción departamentales y un servidor que desempeña las funciones de servidor de dominio Windows, servidor de directorio (DA) y servidor de ficheros.

  Existe un dispositivo NAS que da soporte al servicio de almacenamiento local de ficheros.

  Todos los usuarios disponen de acceso a Internet.

- **Sistema AE** (Internet):

  Es el sistema de información a través del cual se presta el servicio de alojamiento web y sede electrónica municipal.

  Se trata de un sistema externalizado, subcontratado a un proveedor, y que posee una certificación ENS de nivel ALTO para todos los servicios que presta emitido por una entidad certificadora acreditada por ENAC.

- **Ciudadanos** (Internet):

  Se trata del acceso de los ciudadanos desde Internet a los servicios de la Administración Electrónica, los que en nuestro caso están alojados y se publican desde la infraestructura del Sistema **AE**.

En cuanto a las instalaciones, el análisis se centrará en el edificio que es sede principal del ayuntamiento, donde se ubican las oficinas municipales con los puestos de trabajo de tramitación y también el CPD, que aloja el rack principal de la red local, con el servidor de dominio, la electrónica de red y el punto de terminación de red óptica (PTR-O), que es el elemento físico que proporciona acceso a la red de Internet.

3.4.2 Definición del proyecto

Con el propósito de limitar la extensión de este TFM, se ha optado por desarrollar el AR tan solo para el Sistema AE, implementando un único proyecto en PILAR y con un dominio de seguridad.

Con carácter general, aunque podría pensarse que el plantear proyectos por separado para cada sistema no es la mejor opción, sin embargo, al hacerlo de este modo se mantiene una visión unitaria de todos los servicios, información y los activos que le dan soporte al sistema, bajo un único dominio de seguridad. Además, esta elección ofrece un mejor control sobre el comportamiento de la herramienta PILAR que si se tratase de dominios diferentes.

Los parámetros más relevantes configurados para el análisis son los siguientes:

- Valoración = activos + dependencias
- Probabilidad = probabilidad
- Amenazas = mix
- Madurez = madurez
- Modelo de valor = análisis cualitativo
- Fases del proyecto = conectadas
- Dominios de seguridad & fases del proyecto = primero, fase anterior

- Riesgo residual = 4.3
- ENS: índices de madurez y cumplimiento = versión 6

Para un detalle completo del proyecto en PILAR, ver documento adjunto xnaveiroTFM_UOC_01.2022.mgr.

En PILAR los activos se organizan en capas, que son una abstracción que permite organizar los activos de manera que mejore la comprensión del sistema, aunque no repercute en el AR.

Se ha optado por modelar el sistema y los activos en una taxonomía de capas estándar, definiendo posteriormente las dependencias entre activos de manera explícita:

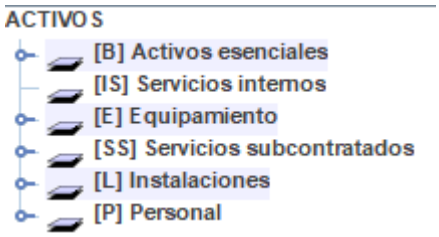


Ilustración 14 Modelo de capas estándar.

Como activos esenciales se crea únicamente ***is [AE] Sistema de Administración electrónica***, que contiene el Servicio de la Sede y la información que maneja dicho servicio y cuyo detalle se observa en la Ilustración 15.

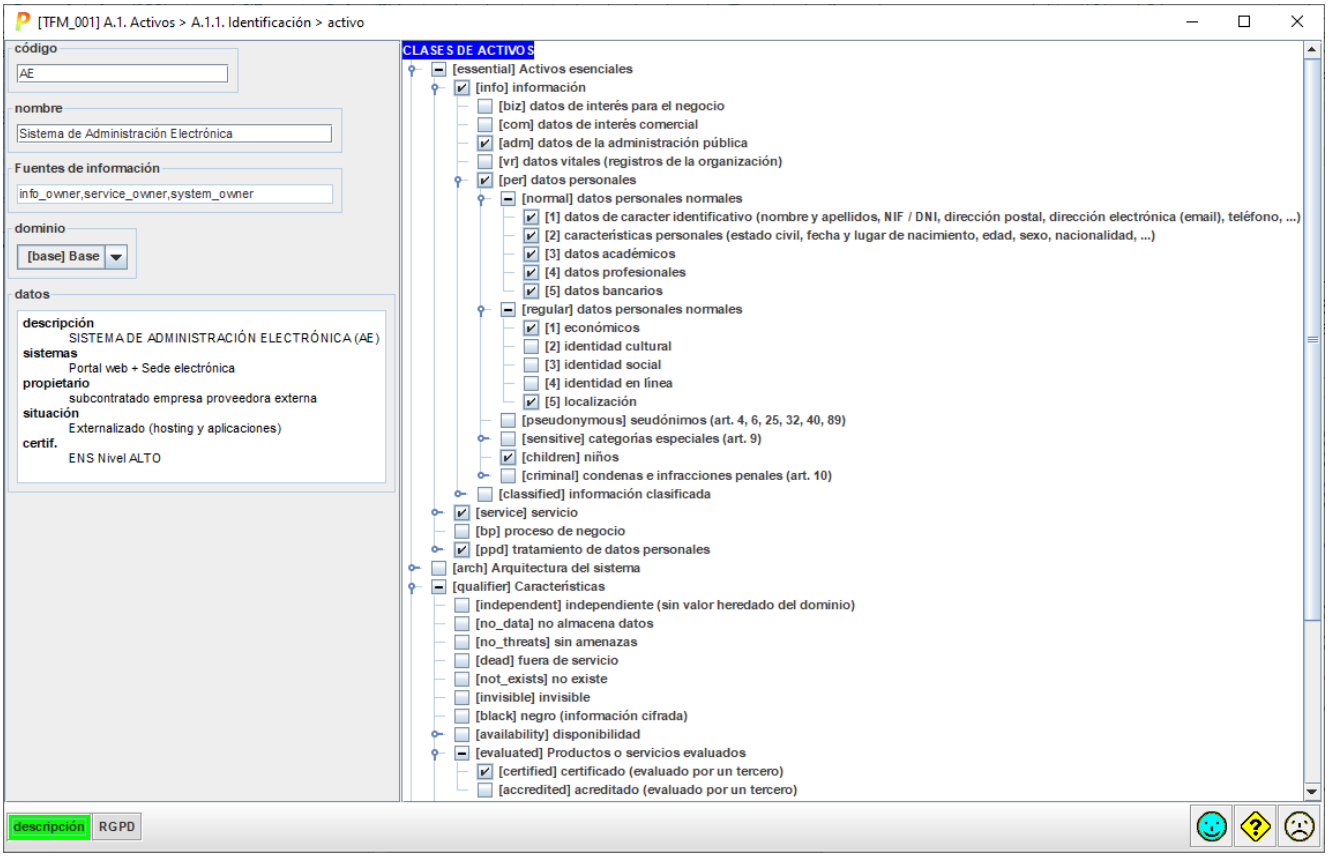


Ilustración 15 Detalle de clases de activos del Sistema [AE].

Como se puede observar, el activo esencial ***[AE]*** contiene a la vez el servicio y la información que maneja dicho servicio, es decir:

- **[adm]** datos de la administración pública

- **[per]** datos personales
  - **[normal]**
  - **[regular]**
  - **[children]**

También se activa el elemento ***[ppd] tratamiento de datos personales***, puesto que los datos que residan en el sistema podrán ser objeto de tratamiento, por ejemplo, a nivel estadístico, para ser integrados en informes estratégicos o en memorias anuales del ayuntamiento.

La capa **[E] Equipamiento** se subdivide en las siguientes:

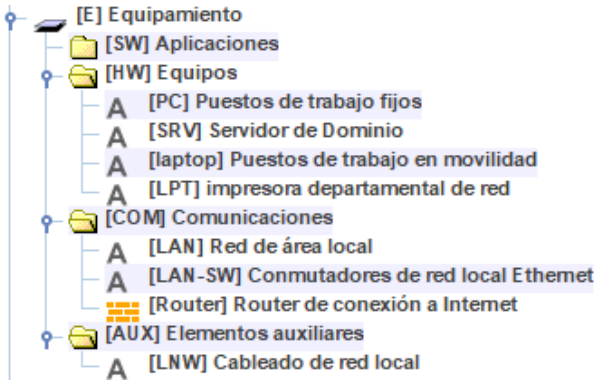


Ilustración 16 Capa [E] Equipamiento.

Dentro de la capa **[SS] Servicios subcontratados**, se han incluido los siguientes elementos:

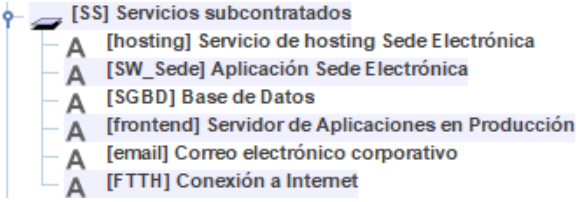


Ilustración 17 Capa [SS] Servicios subcontratados.

Es en esta capa donde se modelan los servicios y aplicaciones subcontratados que conforman el sistema de sede electrónica, además del servicio de correo y la conexión a Internet.

Por último, las capas **[L] Instalaciones** y **[P] Personal** contienen los elementos que se muestran en la siguiente ilustración:

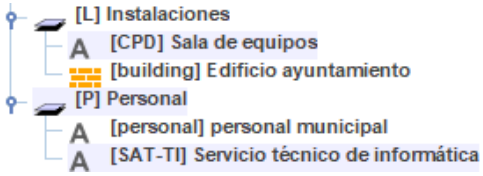


Ilustración 18 Capas [L] Instalaciones y [P] Personal.

Como se ha observado en las anteriores ilustraciones, los activos se agrupan dentro de clases y subclases, unos y otros etiquetados mediante un identificador. Todas estas clases y subclases vienen descritas por la metodología MAGERIT v3 [18].

Basándonos en esta taxonomía de capas, se ha reflejado en ella el modelo de activos para el sistema de información según la configuración recreada para una entidad local descrita en la formulación de nuestro escenario de trabajo.

Capa	Subcapa	Activos
[B] Activos esenciales		[AE] Sistema de Administración Electrónica
[E] Equipamiento	**[HW] Hardware**	[PC] Puestos de trabajo fijos [laptop] Puestos de trabajo en movilidad [LPT] impresora departamental de red [SRV] Servidor de Dominio
	[COM] Comunicaciones	[LAN] Red de área local [LAN-SW] Conmutadores de red local Ethernet [Router] Router de conexión a Internet
	[AUX] Elementos auxiliares	[LNW] Cableado de red local
[SS] servicios subcontratados		[SW_Sede] Aplicación de Sede Electrónica [SGBD] Base de Datos [frontend] Servidor de Aplicaciones [hosting] Servicio de hosting Sede Electrónica [email] Correo electrónico corporativo [FTTH] Conexión a Internet
[L] Instalaciones		[CPD] Sala de equipos [building] Edificio ayuntamiento
[P] Personal		[personal] personal municipal [SAT-TI] Servicio técnico de informática

Tabla 17 Modelo de capas y activos en PILAR.

Siguiendo lo descrito en el apartado 3.4 (Ilustración 11 Reglas para árboles de dependencias.), se han establecido las dependencias debidas entre los diferentes activos, lo que ha generado en el proyecto el mapa de dependencias que se muestra en la Ilustración 19. En este modelo, las capas superiores dependen de las inferiores, en el sentido de que una capa L1 depende de una capa L2 si hay algún activo en L1 que dependa de algún activo en L2.

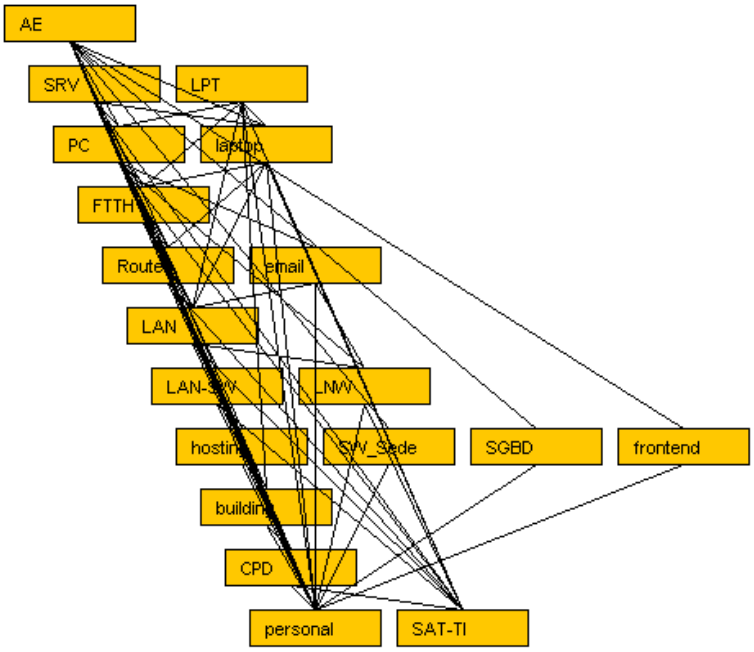


Ilustración 19 Diagrama de dependencias entre activos.

El diagrama de buses que ofrece PILAR muestra otra visión de las dependencias que se han definido entre los diferentes activos:

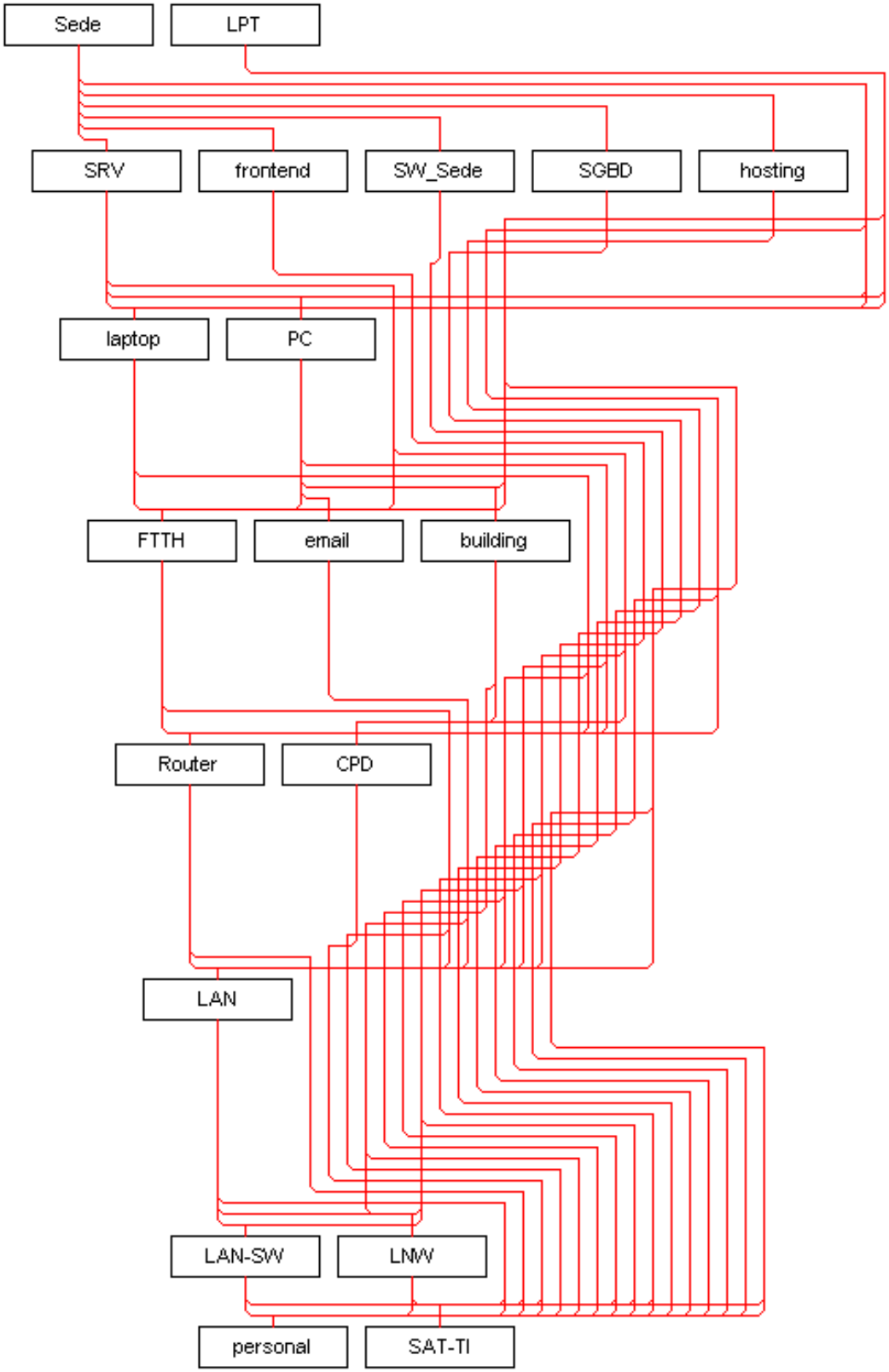


Ilustración 20 Diagrama de buses de dependencias entre activos.

Otra visión diferente de las dependencias lo ofrece el diagra,ma de PILAR de dependencias entre capas:

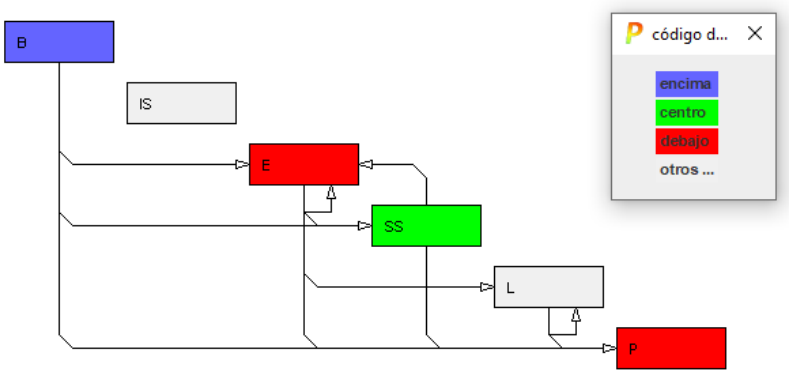


Ilustración 21 Diagrama de dependencias entre capas.

3.4.3 Valoración de los activos

La valoración de un activo desde la perspectiva de la seguridad se relaciona directamente con las medidas de protección que habrá que establecer para protegerlo, de forma que cuanto más valioso es, mayor nivel de protección se requerirá, tendido en cuenta además las dimensiones de seguridad que sean de aplicación en cada activo.

Según lo descrito en el apartado *3.2 Categorización del Sistema*, la categorización del **Sistema AE** que estamos analizando es la siguiente:

Sistema	Confidencialidad [C]	Integridad [I]	Autenticidad [A]	Trazabilidad [T]	Disponibilidad [D]	Nivel Global
SISTEMA DE ADMINISTRACIÓN ELECTRÓNICA (AE)	Medio	Medio	Medio	Bajo	Medio	**Medio**

Tabla 18 Categoría del sistema AE.

Partiendo de esta información, se ha trasladado a la herramienta PILAR la valoración de este activo esencial, y a continuación la propia aplicación, en función de las características y de las dependencias definidas, arrastra dicho valor a los restantes activos en forma de "**valor acumulado**". Esto ofrece una visión sobre el valor de los activos más holística, puesto que el valor propio de un activo puede ser inferior a la suma de los activos que se sitúan por encima de él.

La valoración se ha llevado a cabo cualitativamente, según una serie de niveles que se corresponden con los valores designados en el ENS a las diferentes dimensiones de seguridad:

Valor ENS	Valor PILAR
-	[10] [9]
ALTO	[A+] ALTO+ [A] ALTO [A-] ALTO-
MEDIO	[M+] MEDIO+

	[M] MEDIO [M-] MEDIO-
BAJO	[B+] BAJO+ [B] BAJO
n.a.	[N/A] No Aplicable

Tabla 19 Niveles de valoración de activos ENS/PILAR.

Los valores [9] y [10] de la escala definida en Magerit v3 están fuera del modelo de valoración de ENS.

En la siguiente imagen se muestra el resultado de la valoración de los activos en PILAR. En la línea superior, con fondo blanco se observa la valoración del activo esencial [AE] Sistema de Administración Electrónica, con sus valores propios para cada una de las dimensiones, y en las filas inferiores, con fondo verde, se muestran los valores acumulados de los restantes activos.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[AE] Sistema de Administración Electrónica	[M]	[M]	[B]	[M]	[B]
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[PC] Puestos de trabajo fijos	[B+]	[M]	[B]	[M]	[B]
[SRV] Servidor de Dominio	[M]	[M]	[B]	[M]	[B]
[laptop] Puestos de trabajo en movilidad	[M]	[M]	[B]	[M]	[B]
[LPT] impresora departamental de red	[B]				
[COM] Comunicaciones					
[LAN] Red de área local	[M]	[M]	[B]	[M]	[B]
[LAN-SW] Conmutadores de red local Ethernet	[M]	[M]	[B]	[M]	[B]
[Router] Router de conexión a Internet	[M]	[M]	[B]	[M]	[B]
[AUX] Elementos auxiliares					
[LNW] Cableado de red local	[M]	[M]	[B]	[M]	[B]
[SS] Servicios subcontratados					
[hosting] Servicio de hosting Sede Electrónica	[M]	[M]	[B]	[M]	[B]
[SW_Sede] Aplicación Sede Electrónica	[M]	[M]	[B]	[M]	[B]
[SGBD] Base de Datos	[M]	[M]	[B]	[M]	[B]
[frontend] Servidor de Aplicaciones en Producción	[M]	[M]	[B]	[M]	[B]
[email] Correo electrónico corporativo	[B+]	[M]	[B]	[M]	[B]
[FTTH] Conexión a Internet	[M]	[M]	[B]	[M]	[B]
[L] Instalaciones					
[CPD] Sala de equipos	[M]	[M]	[B]	[M]	[B]
[building] Edificio ayuntamiento	[B+]	[M]	[B]	[M]	[B]
[P] Personal					
[personal] personal municipal	[M]	[M]	[B]	[M]	[B]
[SAT-TI] Servicio técnico de informática	[M]	[M]	[B]	[M]	[B]

Ilustración 22 Valoración de los activos en PILAR.

3.4.4 Amenazas

Tal y como adelantamos cuando definíamos los conceptos fundamentales del AR, al inicio del apartado 3.4:

> Formalmente una **Amenaza** es la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

En este AR se dispone del catálogo de amenazas definidas en MAGERIT v3 e incorporadas a la herramienta PLAR. Están clasificadas en 4 grupos principales ([18]; Libro I, pág. 27):

De origen natural

Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'. Estos defectos se clasifican habitualmente bajo la taxonomía conocida como CVE (Common Vulnerability Enumeration), una norma internacional de facto. La mayor parte de estos defectos suelen afectar a aplicaciones software.

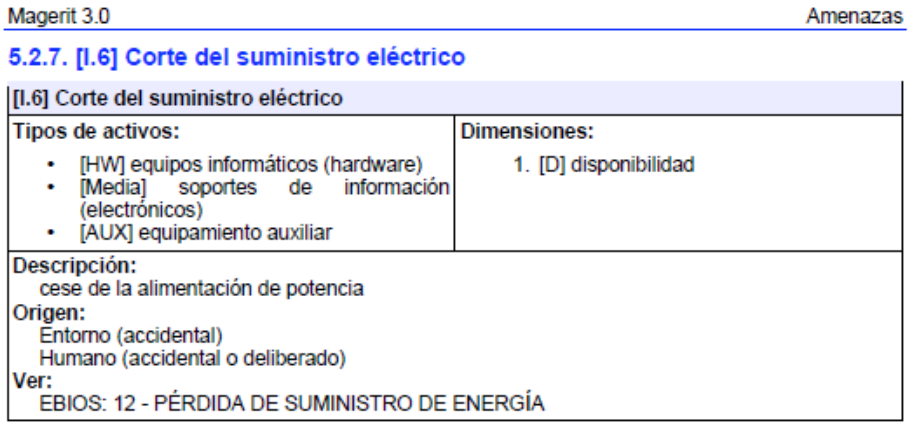
Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

En la siguiente imagen se muestra un ejemplo de caracterización de una amenaza, en este caso para Corte de suministro eléctrico, dentro de la categoría ***[I] De origen industrial***.



Magerit 3.0 Amenazas

5.2.7. [I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

Ilustración 23 Cuadro en Magerit v3 para la amenaza de Corte en suministro eléctrico.

Como se observa en la ilustración anterior, se indican los tipos de activos que están amenazados, la dimensión de seguridad a la que afecta la amenaza e información adicional, como una breve descripción.

Para realizar el AR con PILAR se deben seleccionar las amenazas según la clase de activo de que se trate. La aplicación permite una asociación automática teniendo en cuenta la información asociada a cada activo.

Finalmente, tan solo mencionar que es necesario tener presente que no todas las amenazas afectan a todos los activos, sino que la propia naturaleza y características de cada activo restringen las amenazas a las que está sujeto. En la definición del proyecto se han **desactivado algunas de las amenazas**, por considerarlas irreales en el contexto del análisis de una entidad local como la que se recrea en nuestro escenario de trabajo.

En el grupo de ***[N.*] Desastres naturales*** se omiten:

- ***[N.*.4] Terremotos***
- ***[N.*.5] Tornados***
- ***[N.*.6] Ciclones***
- ***[N.*.9] Tsunamis***
- ***[N.*.10] Tormentas de invierno y frio extremo***
- ***[N.*.11] Calor extremo***
- ***[N.*.12] Volcanes***

Y en el grupo ***[A] Ataques deliberados*** se omiten:

- ***[A.27] Ocupación enemiga***

En la siguiente imagen se observa una ventana de PILAR en la que se explicita la asociación Activo-Amenaza.

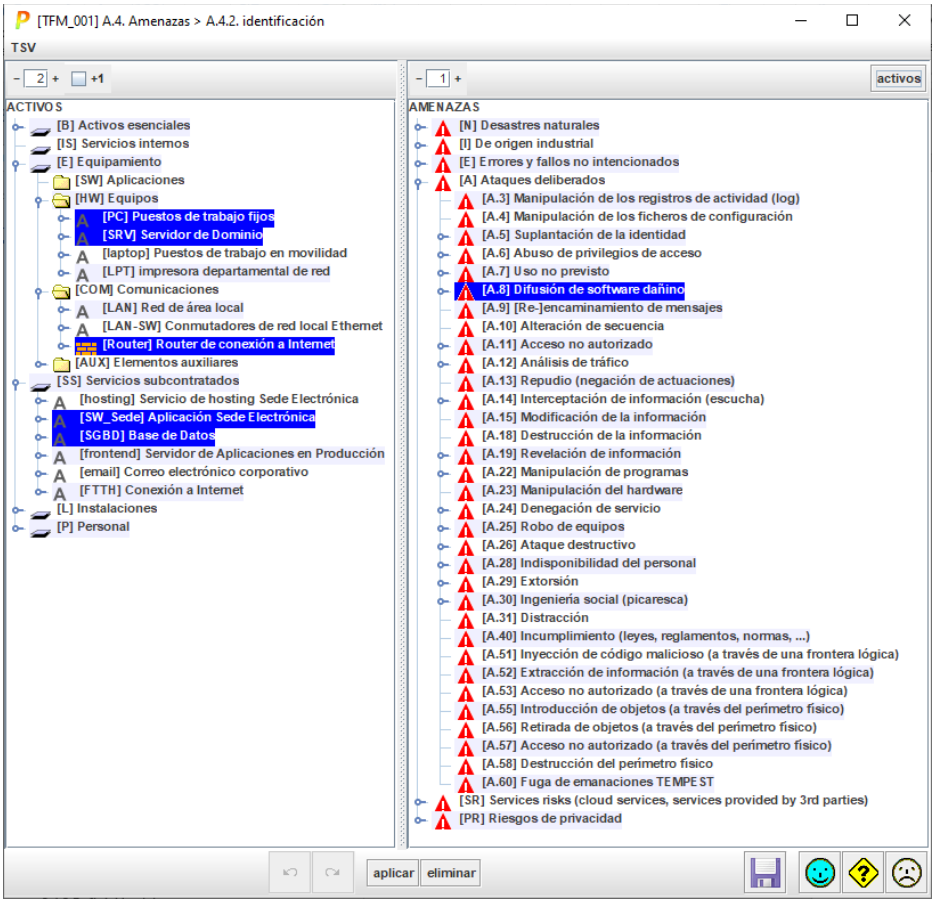


Ilustración 24 Correspondencia entre Amenazas y Activos en PILAR.

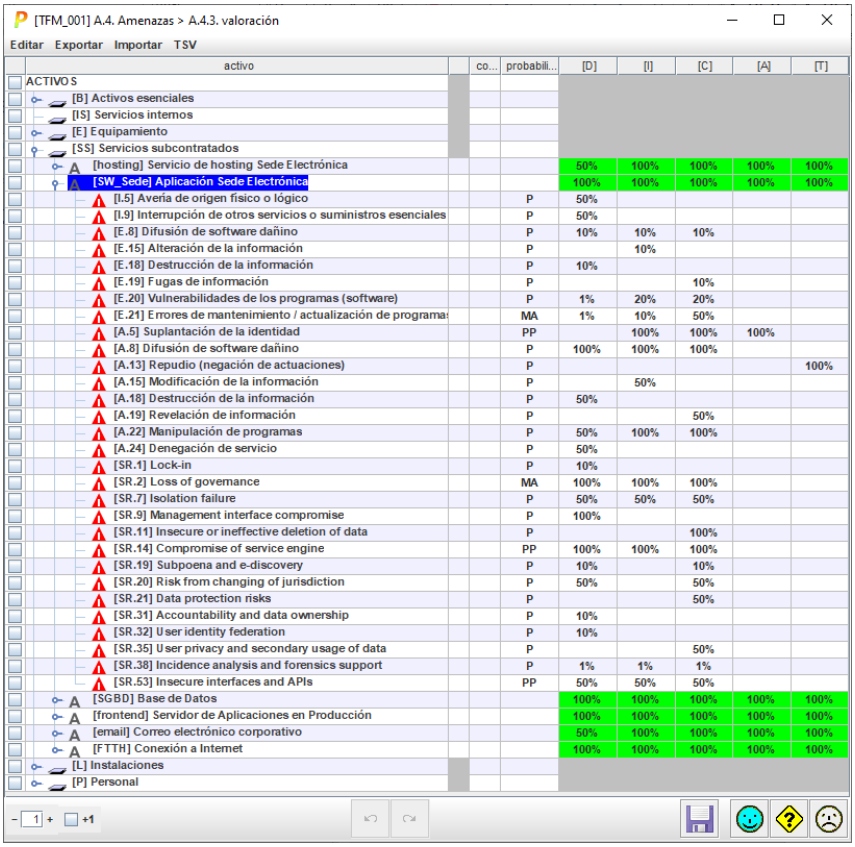
Se puede observar, por ejemplo, que en la ventana anterior se ha seleccionado la amenaza ***[A.8] Difusión de software dañino***, y al pulsar el botón “activos” de la parte superior derecha se resaltan unos determinados activos del sistema, que son los que estarían afectado por dicha amenaza. Esta asociación la realiza de manera automática la propia herramienta PILAR.

La valoración de las amenazas en Magerit se hace según la **frecuencia de ocurrencia** y la **degradación potencial en el valor del activo**:

Frecuencia de ocurrencia	Degradación del valor del activo
CS casi seguro	T – total (100%)
MA muy alta	MA – muy alta (90%)
P posible	A – alta (50%)
PP poco probable	M – media (10%)
MR muy rara	B – baja (1%)

Tabla 20 Valoración de amenazas.

En la siguiente imagen se puede observar la pantalla de PILAR de valoración de amenazas con el ejemplo visible ***[SW_Sede] Aplicación Sede electrónica***.



activo	co...	probabili...	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SS] Servicios subcontratados							
[hosting] Servicio de hosting Sede Electrónica			50%	100%	100%	100%	100%
[SW_Sede] Aplicación Sede Electrónica			100%	100%	100%	100%	100%
[I.5] Avería de origen físico o lógico		P	50%				
[I.9] Interrupción de otros servicios o suministros esenciales		P	50%				
[E.8] Difusión de software dañino		P	10%	10%	10%		
[E.15] Alteración de la información		P		10%			
[E.18] Destrucción de la información		P	10%				
[E.19] Fugas de información		P			10%		
[E.20] Vulnerabilidades de los programas (software)		P	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programa		MA	1%	10%	50%		
[A.5] Suplantación de la identidad		PP		100%	100%	100%	
[A.8] Difusión de software dañino		P	100%	100%	100%		
[A.13] Repudio (negación de actuaciones)		P					100%
[A.15] Modificación de la información		P		50%			
[A.18] Destrucción de la información		P	50%				
[A.19] Revelación de información		P			50%		
[A.22] Manipulación de programas		P	50%	100%	100%		
[A.24] Denegación de servicio		P	50%				
[SR.1] Lock-in		P	10%				
[SR.2] Loss of governance		MA	100%	100%	100%		
[SR.7] Isolation failure		P	50%	50%	50%		
[SR.9] Management interface compromise		P	100%				
[SR.11] Insecure or ineffective deletion of data		P			100%		
[SR.14] Compromise of service engine		PP	100%	100%	100%		
[SR.19] Subpoena and e-discovery		P	10%		10%		
[SR.20] Risk from changing of jurisdiction		P	50%		50%		
[SR.21] Data protection risks		P			50%		
[SR.31] Accountability and data ownership		P	10%				
[SR.32] User identity federation		P	10%				
[SR.35] User privacy and secondary usage of data		P			50%		
[SR.38] Incidence analysis and forensics support		P	1%	1%	1%		
[SR.53] Insecure interfaces and APIs		PP	50%	50%	50%		
[SGBD] Base de Datos			100%	100%	100%	100%	100%
[frontend] Servidor de Aplicaciones en Producción			100%	100%	100%	100%	100%
[email] Correo electrónico corporativo			50%	100%	100%	100%	100%
[FTTH] Conexión a Internet			100%	100%	100%	100%	100%
[L] Instalaciones							
[P] Personal							

Ilustración 25 Valoración de Amenazas en PILAR (A.4.3).

Se puede observar como para la mayoría de las amenazas la probabilidad es “Posible” (P), pero además destacan con una probabilidad “Muy alta” (MA) las dos siguientes, con desigual repercusión en cada una de las dimensiones de seguridad:

- **[E.21]** Errores de mantenimiento / actualización de programas (software)
- **[SR.2]** *Loss of governance*

Se puede consultar el informe de amenazas generado por la herramienta PILAR en el documento adjunto *xnaveiroTFM-01.2022 Informe_amenazas.rtf*.

3.4.5 Identificación y valoración de salvaguardas

Las salvaguardas son los procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que simplemente requieren establecer procedimientos u otro tipo de medidas organizativas para afrontarlas, otras, sin embargo, es necesario abordarlas mediante herramientas tecnológicas (programas o equipos), o incluso algunas necesitarán la adopción de medidas de seguridad física o políticas de personal.

Dentro del proceso de AR, se han de identificar y evaluar las salvaguardas de las que dispone la organización para afrontar las amenazas sobre sus activos. En definitiva, se ha de abordar una auditoría preliminar que permita obtener dicha información.

La aplicación PILAR contempla el catálogo de salvaguardas de MAGERIT v3, agrupadas del siguiente modo:

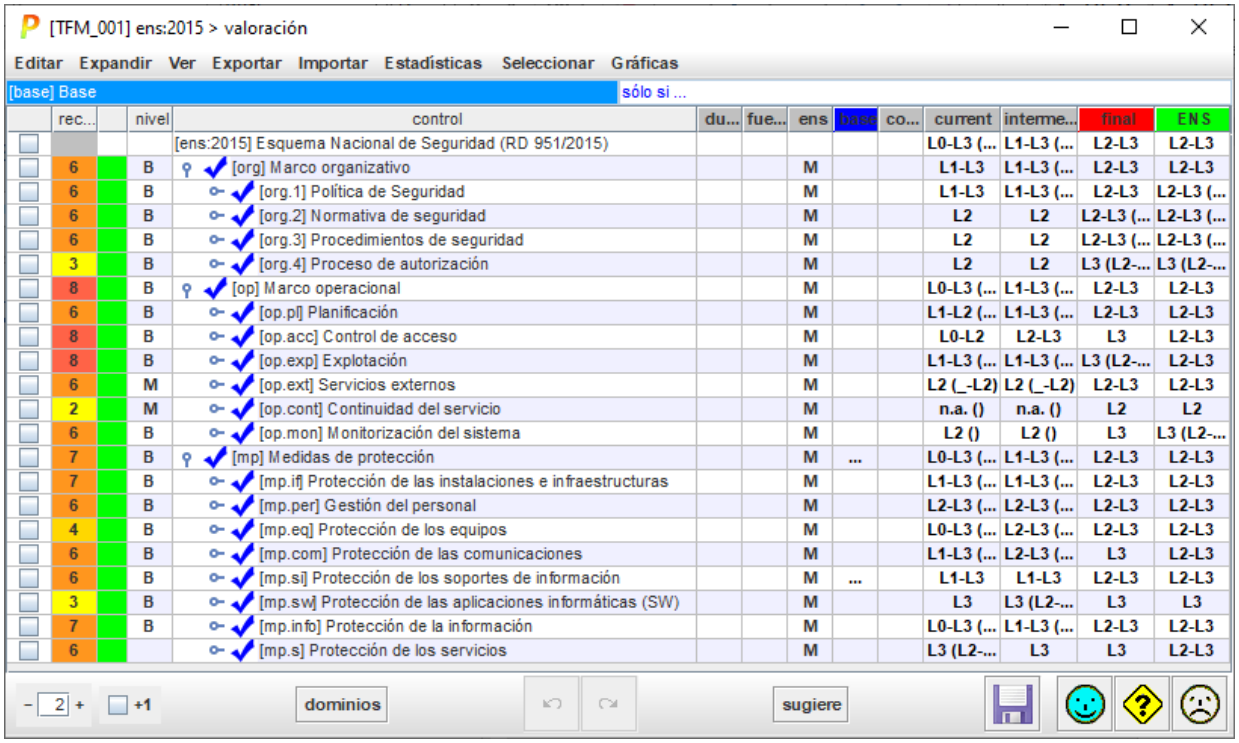
Clasificación	Valores	
Aspecto que trata la salvaguarda	- G: Gestión - T: Técnico - F: seguridad Física - P: gestión del Personal	
Tipo de protección	- PR: prevención - DR: disuasión - EL: eliminación - IM: minimización del impacto - CR: corrección - RC: recuperación - AD: administrativa - AW: concienciación - DC: detección - MN: monitorización - std: norma - proc: procedimiento - cert: certificación o acreditación	
Peso relativo		Máximo (crítica)
		Alto (muy importante)

	Normal (importante)	
	Bajo (interesante)	
	Aseguramiento: componentes certificados	
Recomendación de implantación	- 1 (blanco): no aplica porque no mitigaría ningún riesgo - 2,3 (azul): recomendable - 4,5 (amarillo): bastante recomendable - 6,7 (naranja): muy recomendable - 8,9 (rojo): necesaria	

Tabla 21 Características y clasificación de salvaguardas

En nuestro ejemplo de AR sobre ***[AE] Sistema de Administración electrónica***, se lleva a cabo una valoración de las salvaguardas por fases, según las fases definidas para este proyecto (*current, intermediate, final*), y considerando únicamente el conjunto de controles/salvaguardas denominando **[ens:2015]**. es decir, lo que en términos de PILAR se denomina "***Perfiles de seguridad (EVL)***"

En la siguiente imagen se muestra parcialmente el árbol de valoración, con los controles ens:2015:



rec...		nivel	control	du...	fue...	ens	base	co...	current	interme...	final	ENS
			[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)						L0-L3 (...	L1-L3 (...	L2-L3	L2-L3
6		B	[org] Marco organizativo			M			L1-L3	L1-L3 (...	L2-L3	L2-L3
6		B	[org.1] Política de Seguridad			M			L1-L3	L1-L3 (...	L2-L3	L2-L3 (...
6		B	[org.2] Normativa de seguridad			M			L2	L2	L2-L3 (...	L2-L3 (...
6		B	[org.3] Procedimientos de seguridad			M			L2	L2	L2-L3 (...	L2-L3 (...
3		B	[org.4] Proceso de autorización			M			L2	L2	L3 (L2-...	L3 (L2-...
8		B	[op] Marco operacional			M			L0-L3 (...	L1-L3 (...	L2-L3	L2-L3
6		B	[op.pl] Planificación			M			L1-L2 (...	L1-L3 (...	L2-L3	L2-L3
8		B	[op.acc] Control de acceso			M			L0-L2	L2-L3	L3	L2-L3
8		B	[op.exp] Explotación			M			L1-L3 (...	L1-L3 (...	L3 (L2-...	L2-L3
6		M	[op.ext] Servicios externos			M			L2 (_-L2)	L2 (_-L2)	L2-L3	L2-L3
2		M	[op.cont] Continuidad del servicio			M			n.a. ()	n.a. ()	L2	L2
6		B	[op.mon] Monitorización del sistema			M			L2 ()	L2 ()	L3	L3 (L2-...
7		B	[mp] Medidas de protección			M	...		L0-L3 (...	L1-L3 (...	L2-L3	L2-L3
7		B	[mp.if] Protección de las instalaciones e infraestructuras			M			L1-L3 (...	L1-L3 (...	L2-L3	L2-L3
6		B	[mp.per] Gestión del personal			M			L2-L3 (...	L2-L3 (...	L2-L3	L2-L3
4		B	[mp.eq] Protección de los equipos			M			L0-L3 (...	L2-L3 (...	L2-L3	L2-L3
6		B	[mp.com] Protección de las comunicaciones			M			L1-L3 (...	L2-L3 (...	L3	L2-L3
6		B	[mp.si] Protección de los soportes de información			M	...		L1-L3	L1-L3	L2-L3	L2-L3
3		B	[mp.sw] Protección de las aplicaciones informáticas (SW)			M			L3	L3 (L2-...	L3	L3
7		B	[mp.info] Protección de la información			M			L0-L3 (...	L1-L3 (...	L2-L3	L2-L3
6			[mp.s] Protección de los servicios			M			L3 (L2-...	L3	L3	L2-L3

Ilustración 26 Valoración de salvaguardas ens:2015. PILAR (A.5.2.1).

En la siguiente ilustración se abre el árbol de la imagen anterior, hasta el nivel que permite observar una muestra de la lista de salvaguardas recogidas en PILAR correspondientes *Perfil de seguridad (EVL)* denominado **ens:2015**.

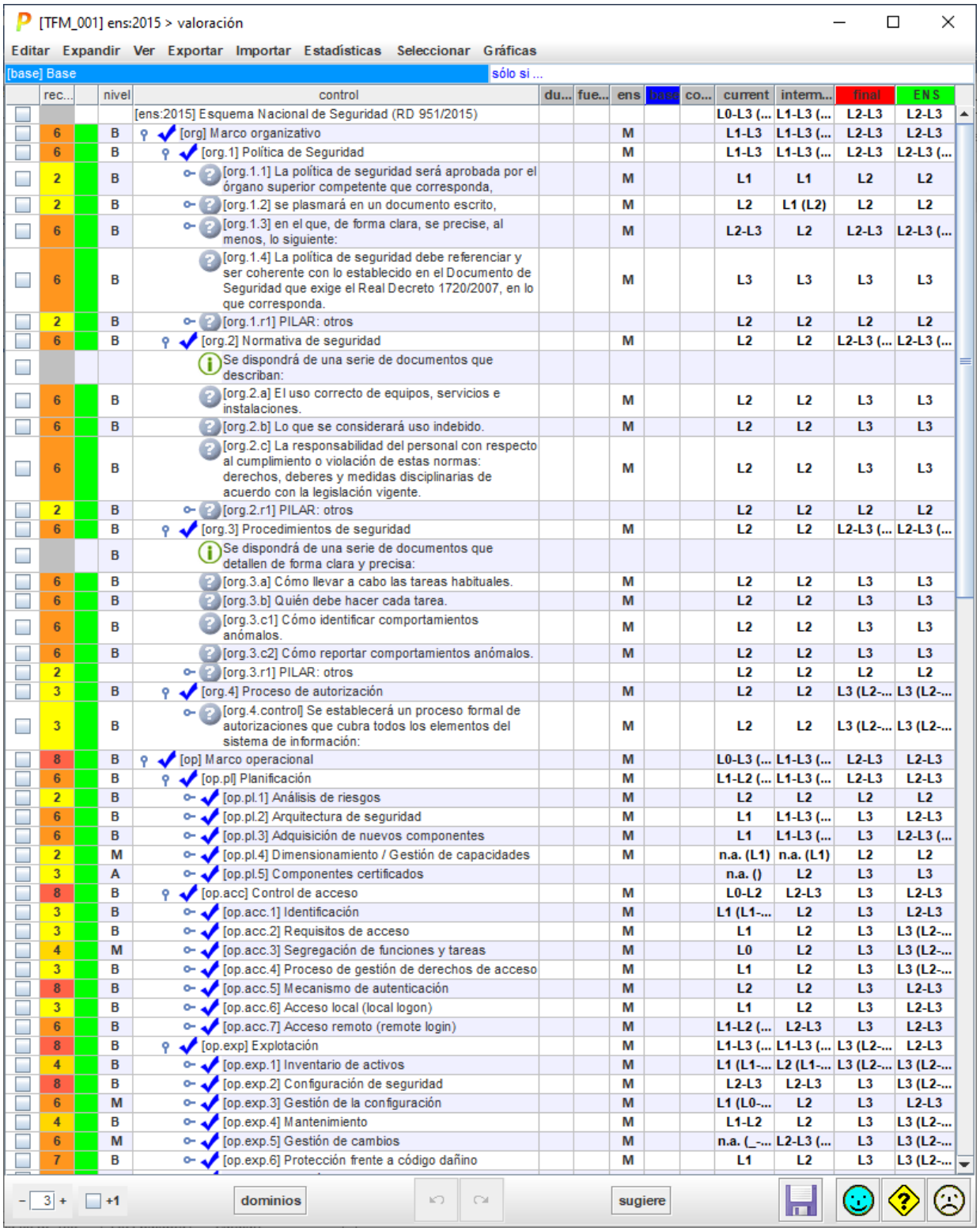


Ilustración 27 Resumen de aplicabilidad de salvaguardas en PILAR (A.5.2.1).

Describimos a continuación los elementos más relevantes que se pueden observar en la ventana anterior.

La primera columna es la de '**recomendación'**. Se trata de una valoración en el rango [1 … 9] estimada por la aplicación PILAR en base al tipo de activo y su valoración en cada dimensión. Además, los valores numéricos se acompañan de un código de colores, descrito en la Tabla 21. También puede aparecer en esta columna las

siguientes marcas en función de la estimación que realiza PILAR sobre esa salvaguarda:

(o) – significa que PILAR opina que es excesiva (“overkill”).

(u) – significa que PILAR opina que es insuficiente (“underkill”).

Si la celda aparece en color gris, significa que esa fila contiene simplemente información o que PILAR no ve justificado poner esa salvaguarda, puesto que a priori no mitigaría ningún riesgo.

Esta columna nos ayuda a la hora de determinar qué salvaguardas se han de priorizar sobre otras, es decir, cuáles se han de poner en marcha en cada fase del proyecto. Cuanto mayor sea el número de la recomendación más prioritaria será la salvaguarda.

La segunda columna (**semáforo**), e indica si la madurez de la salvaguarda es o no suficiente. Como se observa en la Ilustración 26, en nuestro caso siempre se alcanza el valor de madurez requerido por ENS.

El árbol (columna ‘**control’**) puede presentar los siguientes tipos de nodos:

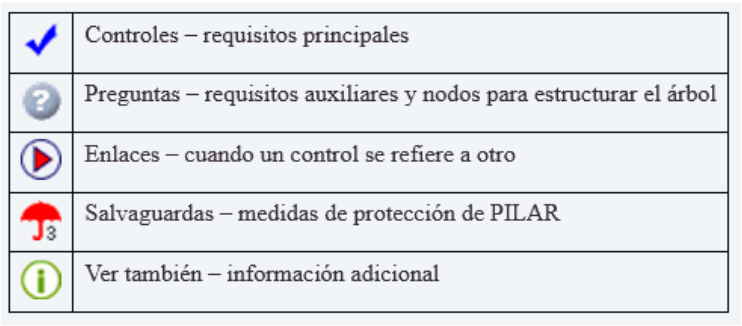


Ilustración 28 Tipos de nodos en valoración de salvaguardas en PILAR (A.5.2.1).

Como se ve en la Ilustración 27, la aplicación asocia los perfiles de seguridad (en este caso ens:2015) a las salvaguardas correspondientes, de manera que el usuario puede estimar el grado de cumplimiento en términos de madurez, según la siguiente escala:

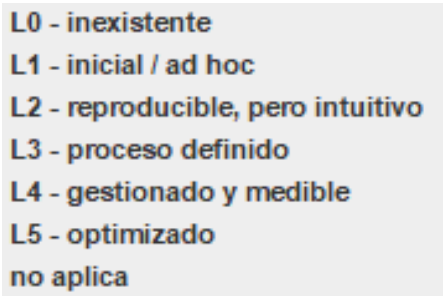


Ilustración 29 Escala de niveles de madurez de salvaguardas en PILAR (A.5.2.1).

Las columnas “*current*”, “*intermediate*” y “*final*” se corresponden con las tres fases definidas para nuestro proyecto de adecuación al ENS:

- “*current*”: situación actual o punto de partida. En esta fase se aplican las medidas únicamente contenidas en el perfil de cumplimiento específico detallado en la Tabla 16. Además, el resultado de la misma aporta la información necesaria para

conocer el gap a nivel de riesgo con relación al ENS las fases posteriores. Al finalizar esta fase se dispone de una autoevaluación documentada que, si el sistema analizado fuese de nivel BÁSICO sería suficiente, sin necesidad de realizar auditorías para la certificación, tal y como se describe en el Anexo III del RD 3/2010 del ENS [4].

- "*intermediate*": estado de aplicación intermedio, en el cual se priorizan las medidas a aplicar en función de las recomendaciones de PILAR y otros factores vinculados a negocio en el contexto del EMC-ENS.
- "*final*": estado final de aplicación de las salvaguardas que, en cualquier caso, ha de coincidir con lo requerido por el ENS, puesto que su cumplimiento y la posterior certificación son los objetivos del Plan de Adecuación.

La columna ENS indica los valores de madurez requeridos por el ENS para cada control/salvaguarda.

Los controles y valores que se han definido obedecen a lo siguientes criterios:

- Únicamente se contemplan los controles y salvaguardas recogidos en ***Perfil de seguridad (EVL)*** denominado **ens:2015**.
- Se realizan las valoraciones para las tres fases contempladas en nuestro proyecto de adecuación al ENS, "*current*", "*intermediate*" y "*final*", descritas anteriormente.
- El punto de partida contempla el cumplimiento tan solo de los controles y en los niveles definidos dentro del **perfil de cumplimiento específico para ayuntamientos de menos de 5.000 habitantes** [7]. Esto permitirá inicialmente emitir un informe de autoevaluación que servirá para conocer las medidas de seguridad implantadas y determinar el gap de seguridad que será necesario recorrer para alcanzar finalmente el cumplimiento del ENS.
- En la segunda fase ("*intermediate*"), se implantan prioritariamente sobre todo las salvaguardas recomendadas por PILAR con puntuación 8 o 9 (color rojo), procurando además que al finalizar esta fase el semáforo de PILAR indique el menor número de controles en rojo.
- El **semáforo** en todos los controles ha de estar en verde para la columna "*final*", es decir, en la última fase del proyecto se alcanza el cumplimiento del ENS.

El nivel de madurez y grado de cumplimiento de partida para el **Sistema AE**, es decir, al inicio de la Fase I ("*current*"), se representa en la siguiente tabla:

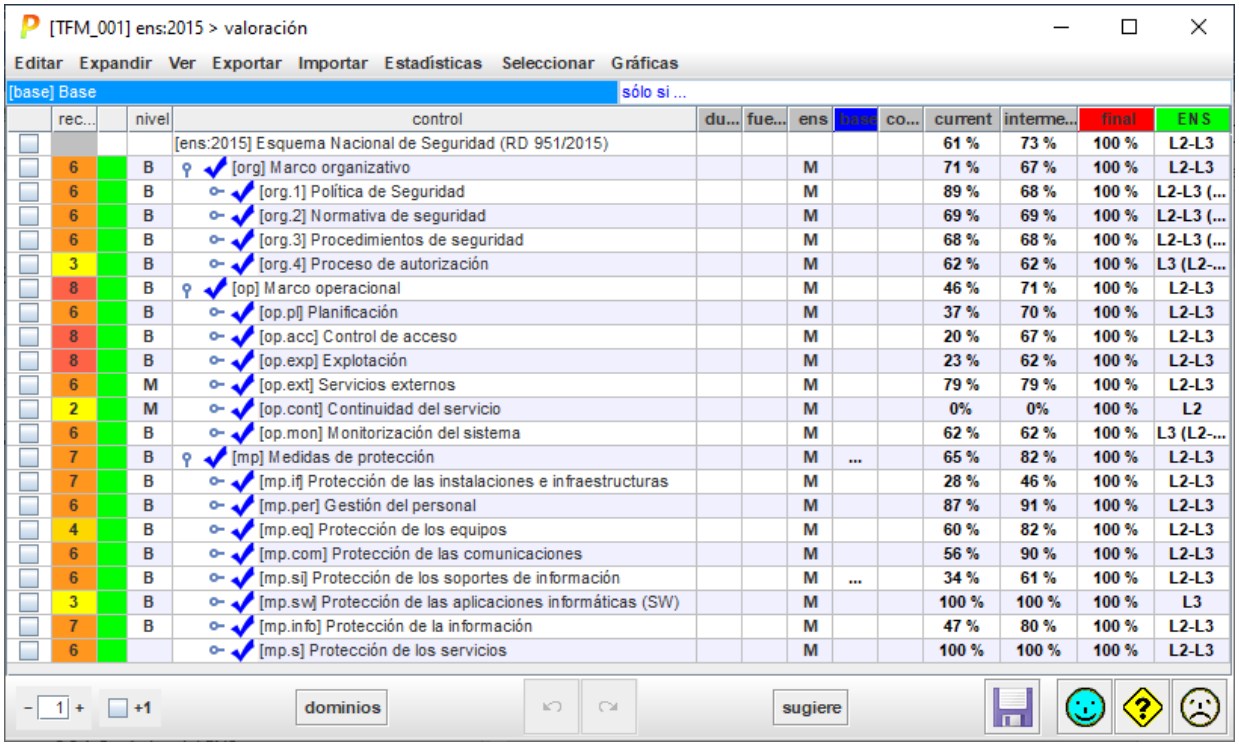
Controles	Nivel de madurez	Porcentaje de cumplimiento ENS
Medidas Organizativas	L0 – L3 (L0 – L1)	11 %
Medidas Operativas	_ - L3	23 %
Medidas de Protección	_ - L3	52 %
Cumplimiento Total	**_ - L3**	**29 %**

Tabla 22 Nivel de madurez y grado de cumplimiento ENS en fase current.

Para una correcta interpretación de los valores de la tabla anterior hay que tener en consideración que cuando el elemento es un control, PILAR distingue entre una **valoración técnica** y una **valoración oficial**. La valoración técnica es calculada por la aplicación en función de las salvaguardas asociadas a ese control, y **se presenta entre paréntesis**. La valoración oficial es la introducida manualmente y se presenta fuera de los paréntesis. Cuando ambas valoraciones coinciden, solo se presenta la oficial. Además, las valoraciones pueden ser un valor sencillo o un rango.

La valoración las salvaguardas en cada una de las fases del proyecto se puede ver de forma más detallada en el documento adjunto *xnaveiroTFM-01.2022 Informe_Evaluacion_Salvaguardas.rtf*.

Se puede observar como una vez aplicadas las medidas indicadas en el perfil de cumplimiento específico, el nivel de madurez global al finalizar la fase *current* es sensiblemente mayor al indicado al inicio de dicha fase, en la Tabla 22.



rec...		nivel	control	du...	fue...	ens	base	co...	current	interme...	final	ENS
			[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)						61 %	73 %	100 %	L2-L3
6		B	[org] Marco organizativo			M			71 %	67 %	100 %	L2-L3
6		B	[org.1] Política de Seguridad			M			89 %	68 %	100 %	L2-L3 (...
6		B	[org.2] Normativa de seguridad			M			69 %	69 %	100 %	L2-L3 (...
6		B	[org.3] Procedimientos de seguridad			M			68 %	68 %	100 %	L2-L3 (...
3		B	[org.4] Proceso de autorización			M			62 %	62 %	100 %	L3 (L2-...
8		B	[op] Marco operacional			M			46 %	71 %	100 %	L2-L3
6		B	[op.pl] Planificación			M			37 %	70 %	100 %	L2-L3
8		B	[op.acc] Control de acceso			M			20 %	67 %	100 %	L2-L3
8		B	[op.exp] Explotación			M			23 %	62 %	100 %	L2-L3
6		M	[op.ext] Servicios externos			M			79 %	79 %	100 %	L2-L3
2		M	[op.cont] Continuidad del servicio			M			0%	0%	100 %	L2
6		B	[op.mon] Monitorización del sistema			M			62 %	62 %	100 %	L3 (L2-...
7		B	[mp] Medidas de protección			M	...		65 %	82 %	100 %	L2-L3
7		B	[mp.if] Protección de las instalaciones e infraestructuras			M			28 %	46 %	100 %	L2-L3
6		B	[mp.per] Gestión del personal			M			87 %	91 %	100 %	L2-L3
4		B	[mp.eq] Protección de los equipos			M			60 %	82 %	100 %	L2-L3
6		B	[mp.com] Protección de las comunicaciones			M			56 %	90 %	100 %	L2-L3
6		B	[mp.si] Protección de los soportes de información			M	...		34 %	61 %	100 %	L2-L3
3		B	[mp.sw] Protección de las aplicaciones informáticas (SW)			M			100 %	100 %	100 %	L3
7		B	[mp.info] Protección de la información			M			47 %	80 %	100 %	L2-L3
6			[mp.s] Protección de los servicios			M			100 %	100 %	100 %	L2-L3

Ilustración 30 Vista de PILAR del nivel de cumplimiento de los controles ENS (A.5.2.1).

Se observa un nivel de cumplimiento global con el ENS de un 61%, lo que implica un nivel de madurez medio-alto en relación a la gestión de la seguridad, identificándose un mayor desarrollo en cuanto a medidas relacionadas con la organización global de la seguridad, algo que resulta lógica dentro del contexto del EMC-ENS (se asume ya desde la fase inicial la política, normativa y procedimientos de seguridad proporcionadas por la entidad superior). El nivel de madurez en las medidas de seguridad que se exigen en la explotación diaria del sistema responde a la ausencia de documentación de la arquitectura de seguridad, de inventario de activos y de la Gestión del cambio, así como la protección frente a código dañino y la Gestión de incidentes.

También es relevante el bajo nivel de madurez en cuanto a los controles de Control de acceso y continuidad del servicio, lo cual es consistente con la aplicación del perfil de cumplimiento específico definido en la Tabla 16.

También se muestra un bajo nivel de madurez en las medidas de protección de las instalaciones e infraestructuras y de los soportes de información.

3.4.6 Impacto y riesgo

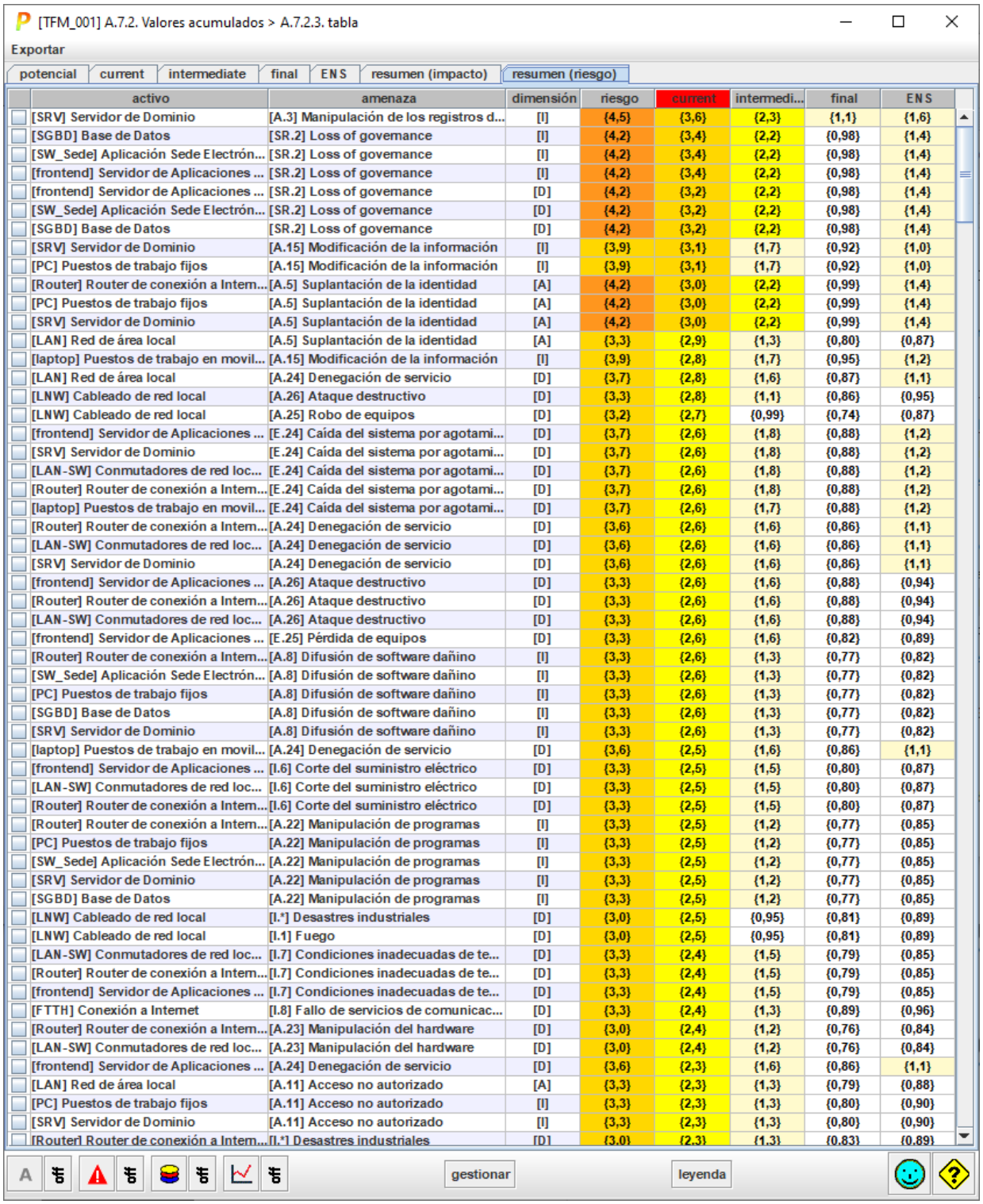
Posteriormente a la valoración de los activos y la aplicación de los niveles de madurez de las salvaguardas, PILAR estima el **riesgo residual**, es decir, el nivel de riesgo que queda después de aplicar el perfil de seguridad definido.

Llegados a este punto, es necesario precisar que no es lo mismo el grado de cumplimiento con el ENS descrito en el apartado 3.4.5 que el riesgo residual resultante de aplicar los niveles de madurez indicados en los controles y salvaguardas.

Los controles requeridos por el RD 3/2010 para un sistema según su categoría y los niveles de seguridad de cada una de las dimensiones han de considerarse como los mínimos exigibles para alcanzar el grado de cumplimiento del ENS, pero al margen de lo anterior pueden considerarse otras medidas de aplicación a nuestro sistema que contribuyan a reducir el riesgo residual.

A este respecto cabe recordar de nuevo que el activo esencial de nuestro sistema está constituido por elementos software y plataformas alojados en infraestructuras externas, y que tanto el software como la infraestructura que los soporta tienen un nivel de seguridad certificado ALTO. Así, por ejemplo, aunque el control **[mp.s.2] Protección de servicios y aplicaciones web**, no se aplicaría según el perfil de cumplimiento específico para ayuntamientos de menos de 5.000 habitantes, en nuestro caso este control tiene un nivel de cumplimiento del 100%. De forma análoga, aunque el control [mp.s.9] Medios alternativos, no es requerido siquiera por el ENS, en nuestro caso la disponibilidad de la Sede Electrónica y del Portal web municipal están garantizadas con recursos alternativos por parte del proveedor externo del servicio (se puede ver en la Ilustración 30 cómo el semáforo de PILAR en ambos controles está en color verde para la fase “*current*”).

En la siguiente imagen se muestra la tabla en PILAR de los valores acumulados de riesgo ordenados por la columna *current*:



activo	amenaza	dimensión	riesgo	current	intermedi...	final	ENS
[SRV] Servidor de Dominio	[A.3] Manipulación de los registros d...	[I]	{4,5}	{3,6}	{2,3}	{1,1}	{1,6}
[SGBD] Base de Datos	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[SW_Sede] Aplicación Sede Electrón...	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[frontend] Servidor de Aplicaciones ...	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[frontend] Servidor de Aplicaciones ...	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SW_Sede] Aplicación Sede Electrón...	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SGBD] Base de Datos	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SRV] Servidor de Dominio	[A.15] Modificación de la información	[I]	{3,9}	{3,1}	{1,7}	{0,92}	{1,0}
[PC] Puestos de trabajo fijos	[A.15] Modificación de la información	[I]	{3,9}	{3,1}	{1,7}	{0,92}	{1,0}
[Router] Router de conexión a Intem...	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[PC] Puestos de trabajo fijos	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[SRV] Servidor de Dominio	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[LAN] Red de área local	[A.5] Suplantación de la identidad	[A]	{3,3}	{2,9}	{1,3}	{0,80}	{0,87}
[laptop] Puestos de trabajo en movil...	[A.15] Modificación de la información	[I]	{3,9}	{2,8}	{1,7}	{0,95}	{1,2}
[LAN] Red de área local	[A.24] Denegación de servicio	[D]	{3,7}	{2,8}	{1,6}	{0,87}	{1,1}
[LNW] Cableado de red local	[A.26] Ataque destructivo	[D]	{3,3}	{2,8}	{1,1}	{0,86}	{0,95}
[LNW] Cableado de red local	[A.25] Robo de equipos	[D]	{3,2}	{2,7}	{0,99}	{0,74}	{0,87}
[frontend] Servidor de Aplicaciones ...	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,8}	{0,88}	{1,2}
[SRV] Servidor de Dominio	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,8}	{0,88}	{1,2}
[LAN-SW] Conmutadores de red loc...	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,8}	{0,88}	{1,2}
[Router] Router de conexión a Intem...	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,8}	{0,88}	{1,2}
[laptop] Puestos de trabajo en movil...	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,7}	{0,88}	{1,2}
[Router] Router de conexión a Intem...	[A.24] Denegación de servicio	[D]	{3,6}	{2,6}	{1,6}	{0,86}	{1,1}
[LAN-SW] Conmutadores de red loc...	[A.24] Denegación de servicio	[D]	{3,6}	{2,6}	{1,6}	{0,86}	{1,1}
[SRV] Servidor de Dominio	[A.24] Denegación de servicio	[D]	{3,6}	{2,6}	{1,6}	{0,86}	{1,1}
[frontend] Servidor de Aplicaciones ...	[A.26] Ataque destructivo	[D]	{3,3}	{2,6}	{1,6}	{0,88}	{0,94}
[Router] Router de conexión a Intem...	[A.26] Ataque destructivo	[D]	{3,3}	{2,6}	{1,6}	{0,88}	{0,94}
[LAN-SW] Conmutadores de red loc...	[A.26] Ataque destructivo	[D]	{3,3}	{2,6}	{1,6}	{0,88}	{0,94}
[frontend] Servidor de Aplicaciones ...	[E.25] Pérdida de equipos	[D]	{3,3}	{2,6}	{1,6}	{0,82}	{0,89}
[Router] Router de conexión a Intem...	[A.8] Difusión de software dañino	[I]	{3,3}	{2,6}	{1,3}	{0,77}	{0,82}
[SW_Sede] Aplicación Sede Electrón...	[A.8] Difusión de software dañino	[I]	{3,3}	{2,6}	{1,3}	{0,77}	{0,82}
[PC] Puestos de trabajo fijos	[A.8] Difusión de software dañino	[I]	{3,3}	{2,6}	{1,3}	{0,77}	{0,82}
[SGBD] Base de Datos	[A.8] Difusión de software dañino	[I]	{3,3}	{2,6}	{1,3}	{0,77}	{0,82}
[SRV] Servidor de Dominio	[A.8] Difusión de software dañino	[I]	{3,3}	{2,6}	{1,3}	{0,77}	{0,82}
[laptop] Puestos de trabajo en movil...	[A.24] Denegación de servicio	[D]	{3,6}	{2,5}	{1,6}	{0,86}	{1,1}
[frontend] Servidor de Aplicaciones ...	[I.6] Corte del suministro eléctrico	[D]	{3,3}	{2,5}	{1,5}	{0,80}	{0,87}
[LAN-SW] Conmutadores de red loc...	[I.6] Corte del suministro eléctrico	[D]	{3,3}	{2,5}	{1,5}	{0,80}	{0,87}
[Router] Router de conexión a Intem...	[I.6] Corte del suministro eléctrico	[D]	{3,3}	{2,5}	{1,5}	{0,80}	{0,87}
[Router] Router de conexión a Intem...	[A.22] Manipulación de programas	[I]	{3,3}	{2,5}	{1,2}	{0,77}	{0,85}
[PC] Puestos de trabajo fijos	[A.22] Manipulación de programas	[I]	{3,3}	{2,5}	{1,2}	{0,77}	{0,85}
[SW_Sede] Aplicación Sede Electrón...	[A.22] Manipulación de programas	[I]	{3,3}	{2,5}	{1,2}	{0,77}	{0,85}
[SRV] Servidor de Dominio	[A.22] Manipulación de programas	[I]	{3,3}	{2,5}	{1,2}	{0,77}	{0,85}
[SGBD] Base de Datos	[A.22] Manipulación de programas	[I]	{3,3}	{2,5}	{1,2}	{0,77}	{0,85}
[LNW] Cableado de red local	[I.*] Desastres industriales	[D]	{3,0}	{2,5}	{0,95}	{0,81}	{0,89}
[LNW] Cableado de red local	[I.1] Fuego	[D]	{3,0}	{2,5}	{0,95}	{0,81}	{0,89}
[LAN-SW] Conmutadores de red loc...	[I.7] Condiciones inadecuadas de te...	[D]	{3,3}	{2,4}	{1,5}	{0,79}	{0,85}
[Router] Router de conexión a Intem...	[I.7] Condiciones inadecuadas de te...	[D]	{3,3}	{2,4}	{1,5}	{0,79}	{0,85}
[frontend] Servidor de Aplicaciones ...	[I.7] Condiciones inadecuadas de te...	[D]	{3,3}	{2,4}	{1,5}	{0,79}	{0,85}
[FTTH] Conexión a Internet	[I.8] Fallo de servicios de comunicac...	[D]	{3,3}	{2,4}	{1,3}	{0,89}	{0,96}
[Router] Router de conexión a Intem...	[A.23] Manipulación del hardware	[D]	{3,0}	{2,4}	{1,2}	{0,76}	{0,84}
[LAN-SW] Conmutadores de red loc...	[A.23] Manipulación del hardware	[D]	{3,0}	{2,4}	{1,2}	{0,76}	{0,84}
[frontend] Servidor de Aplicaciones ...	[A.24] Denegación de servicio	[D]	{3,6}	{2,3}	{1,6}	{0,86}	{1,1}
[LAN] Red de área local	[A.11] Acceso no autorizado	[A]	{3,3}	{2,3}	{1,3}	{0,79}	{0,88}
[PC] Puestos de trabajo fijos	[A.11] Acceso no autorizado	[I]	{3,3}	{2,3}	{1,3}	{0,80}	{0,90}
[SRV] Servidor de Dominio	[A.11] Acceso no autorizado	[I]	{3,3}	{2,3}	{1,3}	{0,80}	{0,90}
[Router] Router de conexión a Intem...	[I.*] Desastres industriales	[D]	{3,0}	{2,3}	{1,3}	{0,83}	{0,89}

Ilustración 31 Vista de PILAR con resumen de riesgo acumulado (A.7.2.3).

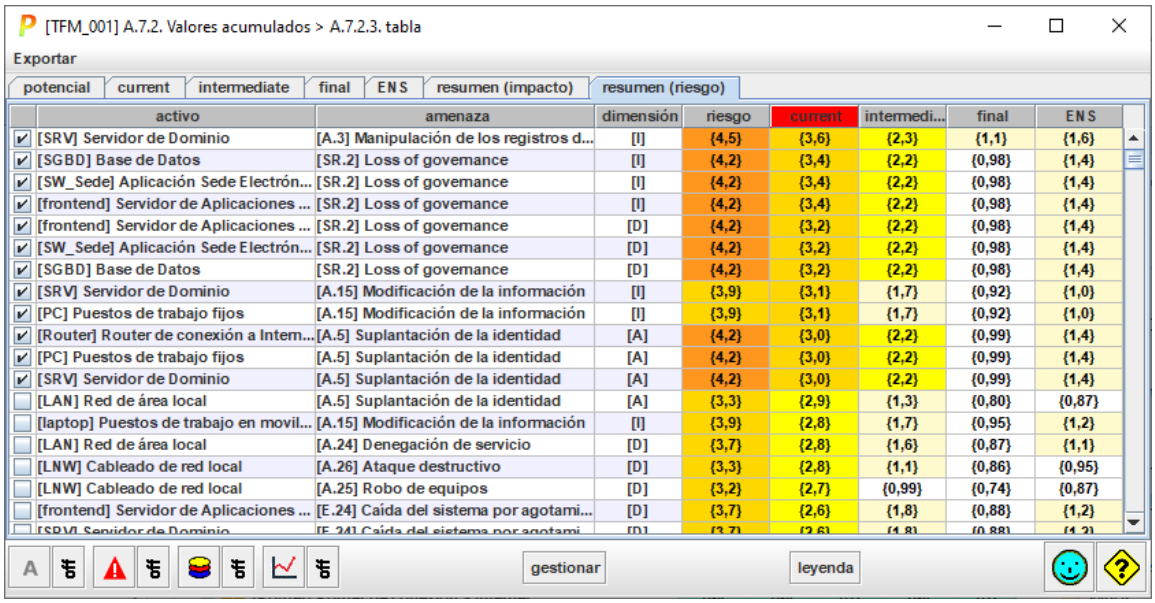
La leyenda de los niveles de riesgo se muestra en la Ilustración 32.

Ilustración 32 Leyenda de niveles de riesgo de PILAR.

La columna “riesgo” muestra el nivel de riesgo potencial, es decir, como si no se hubiese aplicado ninguna medida o salvaguarda.

Al estar seleccionada la columna “*current*”, la tabla se ordena por los valores de dicha columna, de manera que vemos en la parte superior los valores más altos de **riesgo residual** en el sistema AE al remate de la fase inicial, que hemos denominado *current*.

Los responsables de la Información y del Servicio deben aprobar el riesgo residual que conlleve la adopción de las medidas de seguridad correspondientes. Podemos establecer, por ejemplo, que para la entidad local sujeto de nuestro proyecto el organismo certificador, que en este caso será la Diputación Provincial, exige como estado al final de la Fase I (“*current*”) un **nivel de riesgo para los sistemas que ofrecen servicios directamente al público por debajo de {3} – alto**. Para verificar este requerimiento, nuestro ayuntamiento ha de gestionar los riesgos seleccionados en la siguiente imagen:



activo	amenaza	dimensión	riesgo	current	intermedi...	final	ENS
[SRV] Servidor de Dominio	[A.3] Manipulación de los registros d...	[I]	{4,5}	{3,6}	{2,3}	{1,1}	{1,6}
[SGBD] Base de Datos	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[SW_Sede] Aplicación Sede Electrón...	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[frontend] Servidor de Aplicaciones ...	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{2,2}	{0,98}	{1,4}
[frontend] Servidor de Aplicaciones ...	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SW_Sede] Aplicación Sede Electrón...	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SGBD] Base de Datos	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{2,2}	{0,98}	{1,4}
[SRV] Servidor de Dominio	[A.15] Modificación de la información	[I]	{3,9}	{3,1}	{1,7}	{0,92}	{1,0}
[PC] Puestos de trabajo fijos	[A.15] Modificación de la información	[I]	{3,9}	{3,1}	{1,7}	{0,92}	{1,0}
[Router] Router de conexión a Intem...	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[PC] Puestos de trabajo fijos	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[SRV] Servidor de Dominio	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{2,2}	{0,99}	{1,4}
[LAN] Red de área local	[A.5] Suplantación de la identidad	[A]	{3,3}	{2,9}	{1,3}	{0,80}	{0,87}
[laptop] Puestos de trabajo en movil...	[A.15] Modificación de la información	[I]	{3,9}	{2,8}	{1,7}	{0,95}	{1,2}
[LAN] Red de área local	[A.24] Denegación de servicio	[D]	{3,7}	{2,8}	{1,6}	{0,87}	{1,1}
[LNW] Cableado de red local	[A.26] Ataque destructivo	[D]	{3,3}	{2,8}	{1,1}	{0,86}	{0,95}
[LNW] Cableado de red local	[A.25] Robo de equipos	[D]	{3,2}	{2,7}	{0,99}	{0,74}	{0,87}
[frontend] Servidor de Aplicaciones ...	[E.24] Caída del sistema por agotami...	[D]	{3,7}	{2,6}	{1,8}	{0,88}	{1,2}

Ilustración 33 Selección de los niveles de riesgo a tratar.

La propia aplicación PILAR, pulsando en el botón “**gestionar**” nos devuelve a la pantalla de valoración (A.5.2.1), donde podemos incrementar el nivel de madurez de las

medidas necesarias para reducir el nivel de riesgo residual hasta niveles aceptables en los términos que nos exige la entidad certificadora.

A modo de ejemplo, en la Ilustración 34 se observan las sugerencias relacionadas con el control **[op.acc.3] Segregación de funciones y tareas** cuando se activa la opción en PILAR mediante el botón "**sugiere**". En la parte inferior aparecen una serie de salvaguardas **ordenadas según el orden en que PILAR sugiere que se mejore su valoración en la fase seleccionada**. Esto facilita el revisar e implantar o incrementar el nivel de madurez de las medidas para reducir el nivel de riesgo residual.

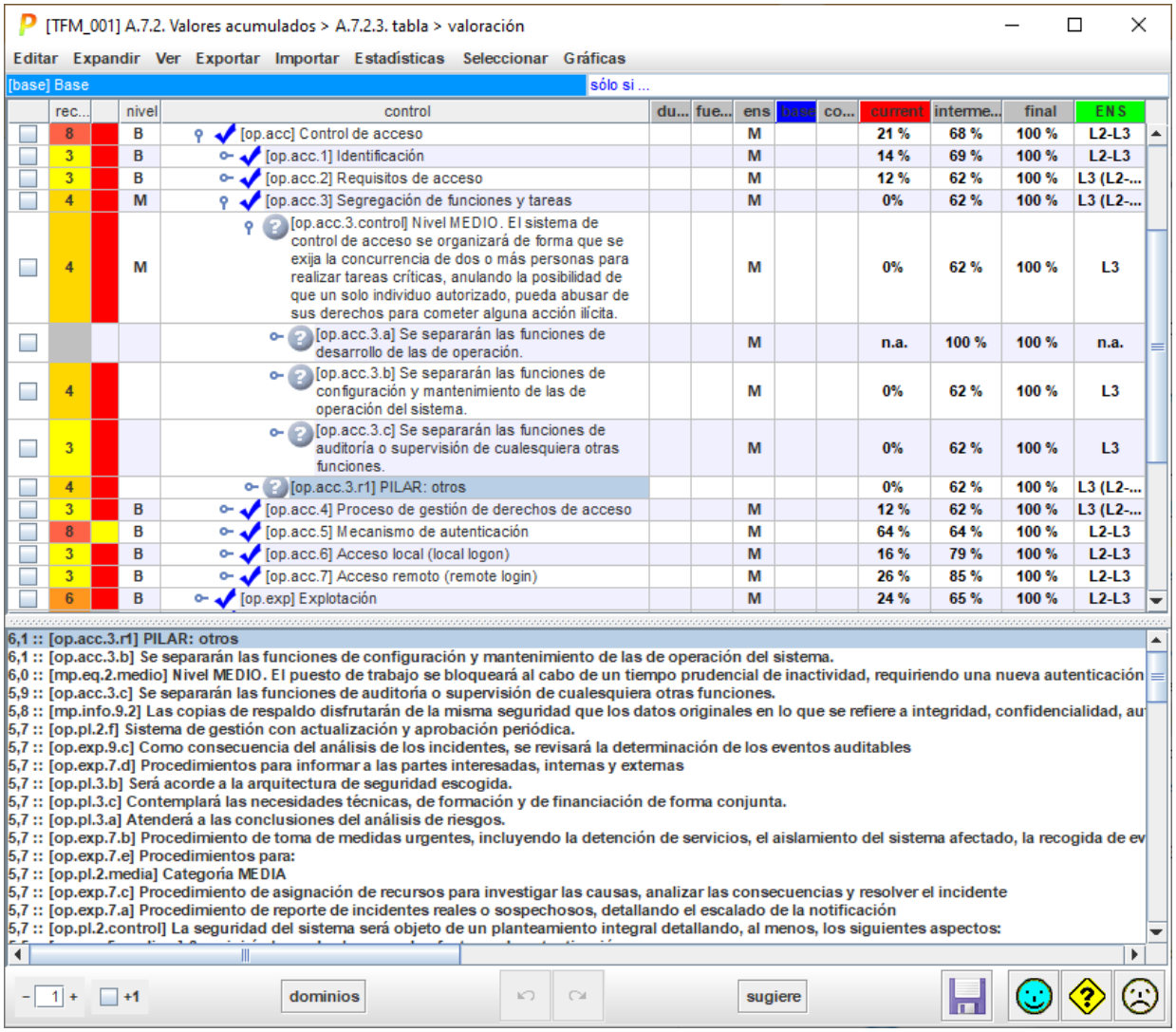


Ilustración 34 Ventana PILAR de valoración de medidas y salvaguardas.

Tal y com se observa en la imagen anterior, en esta ventana es posible seleccionar una de las sugerencias, por ejemplo, las que ofrecen una mayor puntuación estimada por la herramienta, y así, para cada una de las fases del proyecto, por ejemplo "*current*". ajustar el nivel de madurez de la salvaguarda.

Se puede consultar el informe de insuficiencias que se obtiene de PILAR de cada una de as fases del proyecto en el documento adjunto *xnaveiroTFM-01.2022 Informe_insuficiencias.rtf*.

El siguiente gráfico describe visualmente la situación de cumplimiento en cada una de las familias de medidas ENS para cada fase de nuestro proyecto.

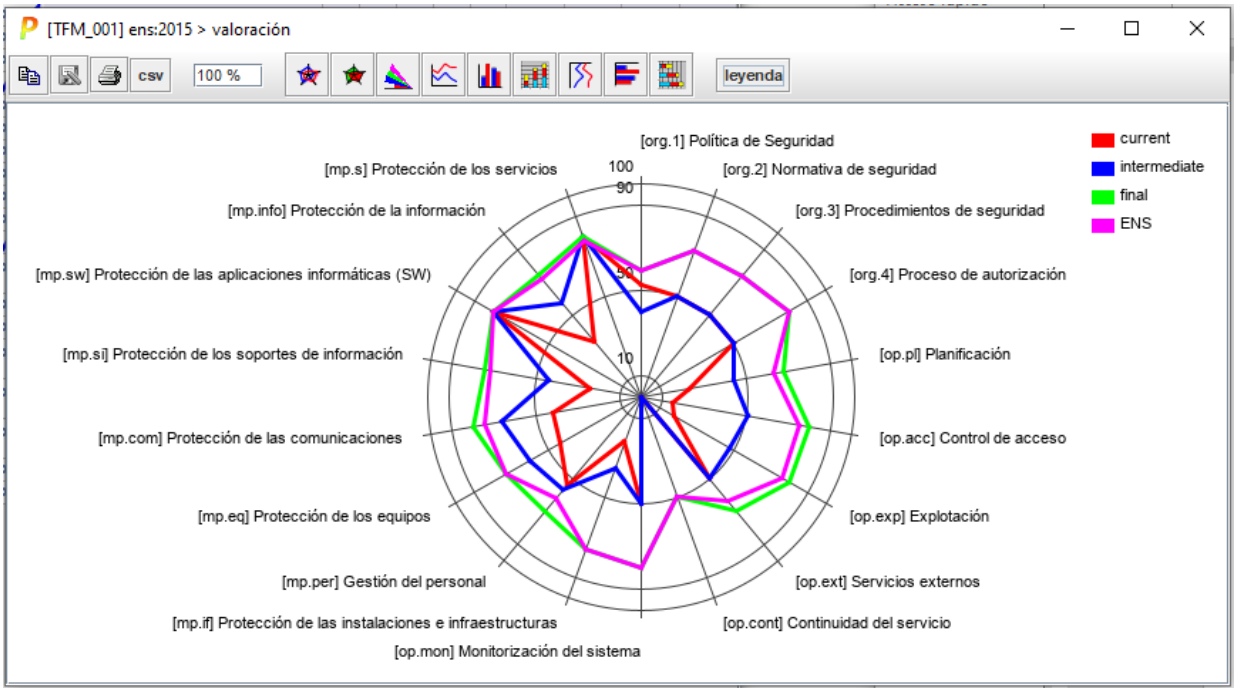


Ilustración 35 Diagrama PILAR de porcentajes de cumplimiento ENS en cada familia de medidas y en cada fase del proyecto.

Se observa en el gráfico cómo el nivel de cumplimiento con el ENS se va incrementando de una fase a otra hasta la fase final, en la que se consigue el cumplimiento total de las medidas requeridas por el ENS.

El informe con los valores obtenidos para el AR se puede consultar en el documento adjunto *xnaveiroTFM-01.2022 Informe_AR.rtf*.

3.5 Plan de mejora de la seguridad

Una vez llevado a cabo el AR inicial y analizadas sus conclusiones, se ha de abordar la elaboración de un plan de mejora de la seguridad que contenga las actuaciones necesarias para mejorar todas las áreas en las que se han identificado margen de mejora, con el objetivo final de alcanzar el cumplimiento del ENS.

Dicho plan se estructura siguiendo las fases definidas a anteriormente para nuestro proyecto: "*current*", "*intermediate*" y "*final*":

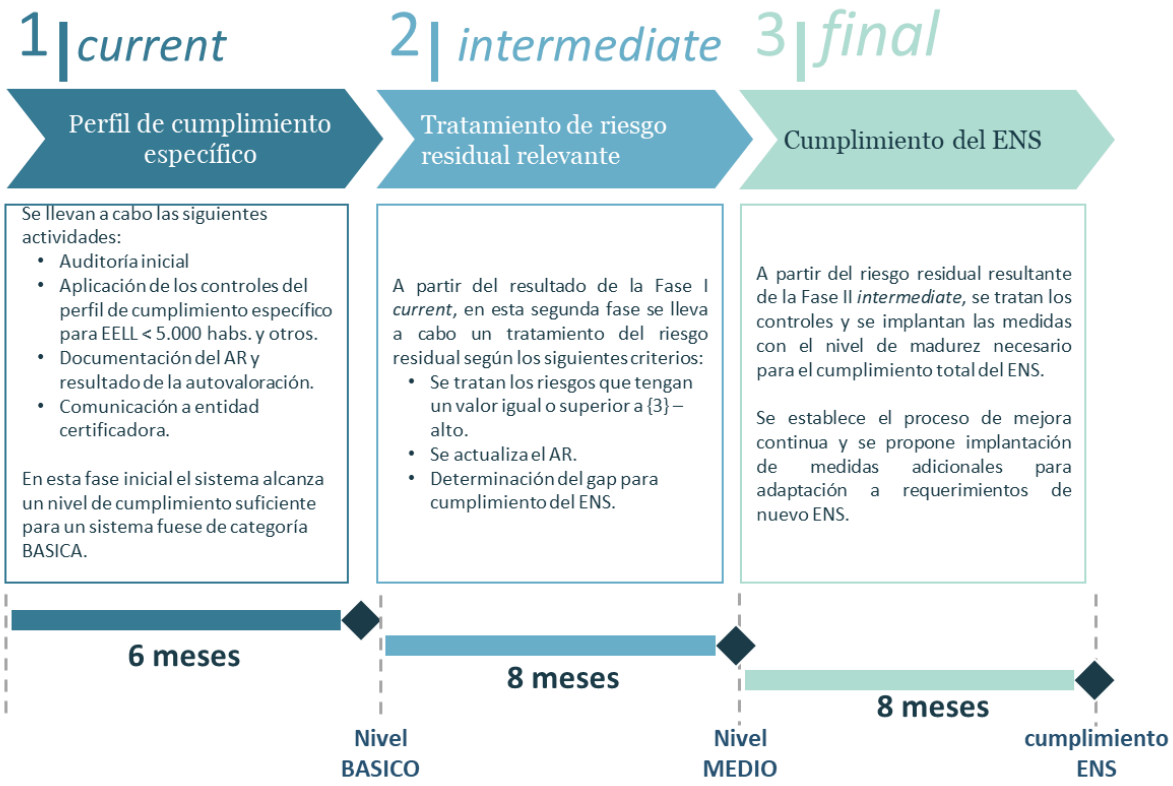


Ilustración 36 Distribución del Pan de mejora de la seguridad según las fases del proyecto.

A continuación, se indica con cierto nivel de detalle las principales acciones a llevar a cabo en cada una de estas fases.

Fase I *current*

Se aplican al menos los controles definidos en el perfil de cumplimiento específico para entidades locales de menos de 5.000 habitantes [7]. El detalle de las medidas aplicadas durante esta primera fase se explica en la siguiente tabla:

Control/Salvaguarda	Nivel de madurez	Porcentaje de cumplimiento ENS	Observaciones
Marco organizativo			
[org.1] Política de seguridad	L2	99 %	A falta de la aprobación final por parte de la entidad certificadora

Control/Salvaguarda	Nivel de madurez	Porcentaje de cumplimiento ENS	Observaciones
[org.2] Normativa de seguridad	L2	69%	Se asume la normativa de seguridad que el organismo superior (entidad certificadora) requiere.
[org.3] Procedimientos de seguridad	L2	68%	La implantación de este control se apoya en los procedimientos definidos por organismo superior (entidad certificadora).
[org.4] Procedimientos de seguridad	L2	62%	Se implanta el proceso formal de autorizaciones.
Marco operacional			
[op.pl] Planificación	L1 – L2	34%	Se implantan los controles [op.pl.1], [op.pl.2] y [op.pl.3]
[op.acc] control de acceso	L0 – L2	19%	Se implantan los controles [op.acc.1], [op.acc.2], [op.acc.4], [op.acc.5], [op.acc.6], [op.acc.7]
[op.exp] Explotación	L1 – L3	23%	Se implantan los controles [op.exp.1], [op.exp.2], [op.exp.4], [op.acc.6], [op.exp.7], [op.exp.8], [op.exp.9], [op.exp.11]
[op.ext] Servicios externos	L2	79%	Se implantan los controles [op.ext.1], [op.ext.2]
[op.mon] Monitorización del sistema	L2	62%	Se implantan el control [op.mon.2].
Medidas de protección			
[mp.if] Protección de las instalaciones e infraestructuras	L1 – L3	100%	Se implantan los controles [mp.if.1], [mp.if.2], [mp.if.3], [mp.if.4], [mp.if.5], [mp.if.7]
[mp.per] Gestión del personal	L2 – L3	79%	Se implantan los controles [mp.per.2], [mp.per.3], [mp.per.4]
[mp.eq] Protección de los equipos	L0 – L3	100%	Se implantan los controles [mp.eq.1], [mp.eq.3]
[mp.com] Protección de las comunicaciones	L1 – L3	52%	Se implantan los controles [mp.com.1], [mp.com.2], mp.com.3]
[mp.si] Protección de los soportes de información	L1 – L3	30%	Se implantan los controles [mp.si.1], [mp.si.2], [mp.si.3], [mp.si.4], [mp.si.5]
[mp.sw] Protección de las aplicacines informáticas (SW)	L3	100%	A pesar de que estos controles no son requeridos por el perfil de cumplimiento específico que se aplica, y que la entidad local no desarrolla aplicaciones con recursos propios, la organización exige a los contratistas proveedores de software que en un plazo razonable de tiempo presenten las certificaciones debidas del ENS sobre sus productos y/o servicios.

Control/Salvaguarda	Nivel de madurez	Porcentaje de cumplimiento ENS	Observaciones
[mp.info] Protección de la información	L0 - L3	42%	Se implantan los controles [mp.info.1], [mp.info.2], [mp.info.4], [mp.info.5], [mp.info.6]. Además, y aun cuando el perfil de cumplimiento específico que se aplica no lo requiere, la organización tiene implantado el control [mp.info.9] Copias de seguridad.
[mp.s] Protección de los servicios	L3	100%	Se implanta el control [mp.s.1]. Además, y aun cuando el perfil de cumplimiento específico que se aplica no lo requiere, la organización tiene implantado el control [mp.s.2] Protección de servicios y aplicaciones web, puesto que el sistema AE analizado es proporcionado por un proveedor externo que acredita una certificación ENS de nivel ALTO.

Tabla 23 Medidas aplicadas en la fase current.

Fase II *intermediate*

En esta segunda fase, partiendo del riesgo residual que se obtiene al final de la fase anterior se aplican los niveles de madurez necesarios como para reducir ese nivel de riesgo a un valor por debajo de {3} – alto, que es el nivel aceptado por el organismo superior (entidad certificadora) para esta fase intermedia previa al cumplimiento total del ENS. En la siguiente imagen se observan los activos sometidos a amenzas con un nivel de riesgo alto en la fase "*intermediate*".

potencial | current | intermediate | final | ENS | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	riesgo	current	intermediate	final	ENS
[SRV] Servidor de Dominio	[A.3] Manipulación de los registros de...	[I]	{4,5}	{3,6}	{3,4}	{1,1}	{1,6}
[SW_Sede] Aplicación Sede Electrónica	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{3,3}	{0,97}	{1,4}
[SGBD] Base de Datos	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{3,3}	{0,97}	{1,4}
[frontend] Servidor de Aplicaciones e...	[SR.2] Loss of governance	[I]	{4,2}	{3,4}	{3,3}	{0,97}	{1,4}
[SW_Sede] Aplicación Sede Electrónica	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{3,2}	{0,97}	{1,4}
[SGBD] Base de Datos	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{3,2}	{0,97}	{1,4}
[frontend] Servidor de Aplicaciones e...	[SR.2] Loss of governance	[D]	{4,2}	{3,2}	{3,2}	{0,97}	{1,4}
[SRV] Servidor de Dominio	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{3,1}	{0,98}	{1,4}
[PC] Puestos de trabajo fijos	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{3,1}	{0,98}	{1,4}
[Router] Router de conexión a Internet	[A.5] Suplantación de la identidad	[A]	{4,2}	{3,0}	{3,1}	{0,98}	{1,4}

Ilustración 37 Activos con nivel de riesgo alto en la fase intermediate.

Apoyándose en las funciones de asistencia de PILAR (recomendación, semáforo y sugerencias) tal y como se observa en la Ilustración 38, en esta Fase II se actualizan los niveles de madurez de los controles indicados como más prioritarios.

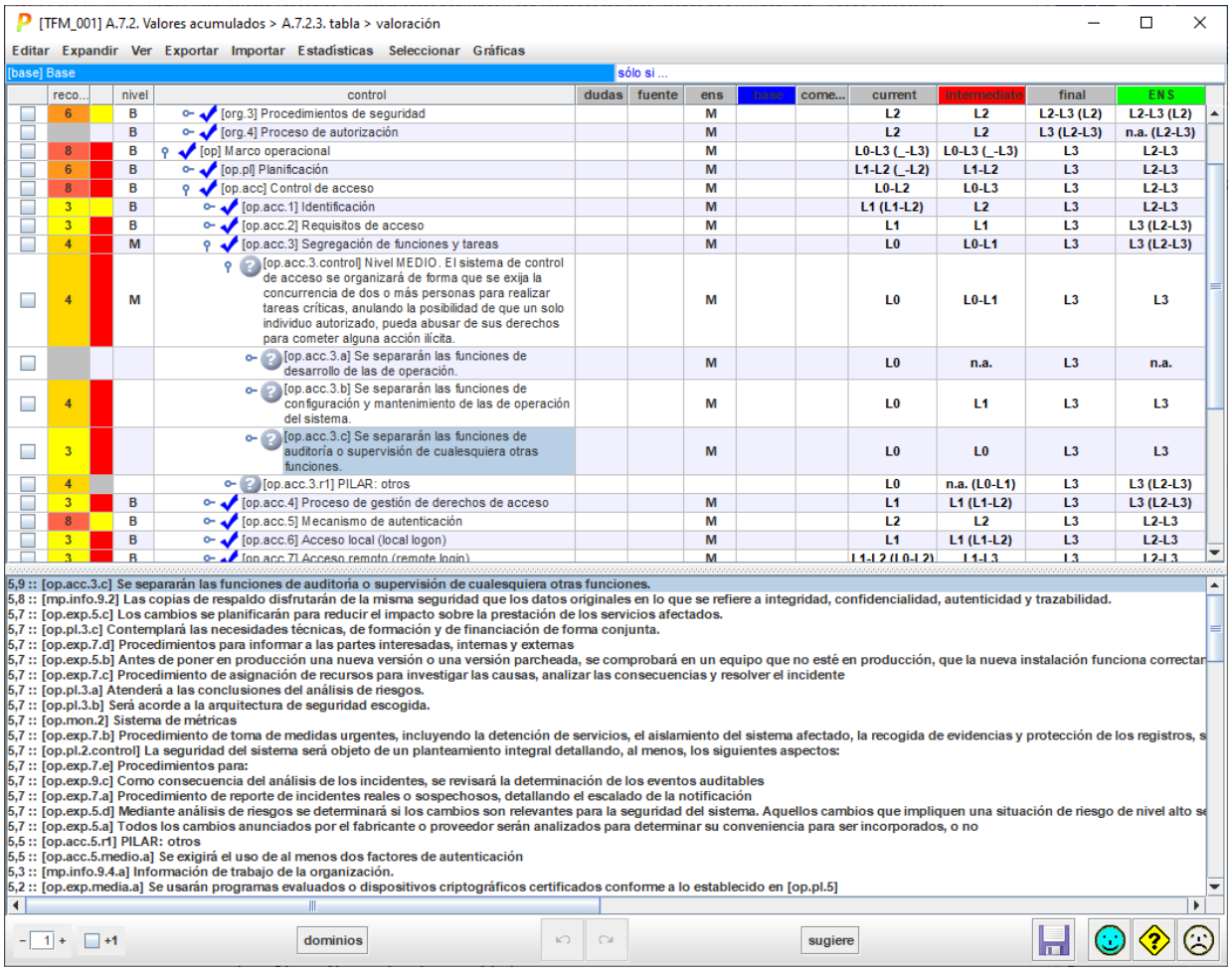


Ilustración 38 Pantalla de Pilar con sugerencias, semáforo y puntuación de recomendación.

Como resultado de la mejora en el nivel de madurez a todas las medidas que mantienen el semáforo en rojo para esta segunda fase, se obtienen los siguientes niveles de riesgo:

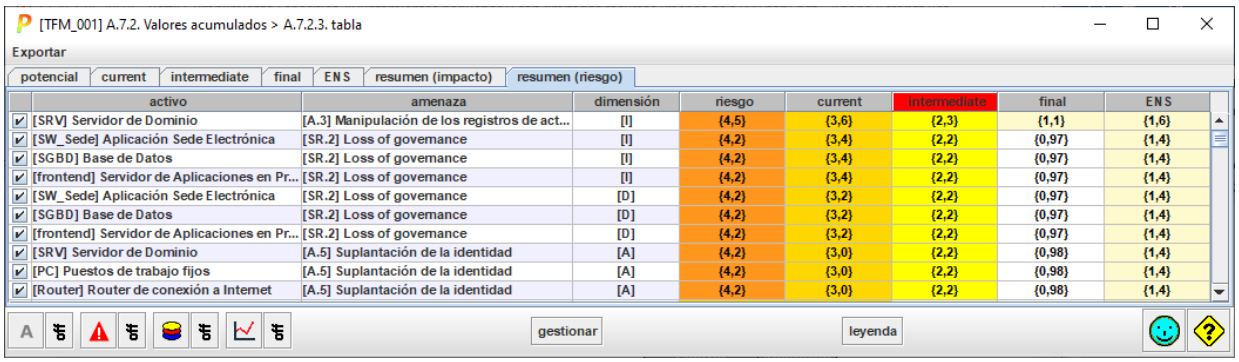


Ilustración 39 Resultado del tratamiento de riesgo durante la fase intermediate.

Fase III *intermediate*

Esta fase tiene por objetivo alcanzar el cumplimiento total del ENS. Para ello, tal y como se hizo en la fase anterior, partiendo del AR y utilizando las funciones de asistencia de PILAR se implantan las medidas con el nivel requerido por el ENS.

Como se observa en la Ilustración 39, el riesgo acumulado en la fase "*final*" es inferior al definido para ENS.

Las medidas que en esta fase "*final*" contribuyen al cumplimiento del ENS de manera más relevante con la actualización en su nivel de madurez se resumen en la siguiente tabla.

Control/Salvaguarda	Nivel de madurez en fase *intermediate*	Porcentaje cumplimiento ENS en fase *intermediate*	Observaciones
Marco operacional			
[op.acc] Control de acceso	L2 – L3	67%	El control más relevante es el [op.acc.5] Mecanismo de autenticación.
[op.exp] Explotación	L1 – L3	62%	Los controles más relevantes en esta familia son: - [op.exp.2] Configuración de seguridad. - [op.exp.6] Protección frente a código dañino.
Medidas de protección			
[mp.if] Protección de las instalaciones e infraestructuras	L1 – L3	82%	El control más relevante es el [mp.if.5] Áreas separadas y con control de acceso.
[mp.info] Protección de la información	L1 - L3	80%	El control más relevante es el [mp.info.9] Copias de seguridad.

Tabla 24 Medidas más relevantes actualizadas en la fase final.

4 Conclusiones

Partiendo de la 7ª edición del informe INES, 2020 (fuente [11]), el nivel de cumplimiento del ENS se sitúa en:

- 64,93% en sistemas de categoría ALTA.
- 68,24% en sistemas de categoría MEDIA
- 84% en sistemas de categoría BÁSICA

A la vista de estos resultados, y revisando además la información facilitada por CCN-CERT sobre ***Sector Público Certificado*** [22] (por ejemplo, en cuanto a entidades locales solo figuran 9 certificadas), se concluye que **es necesario mantener el esfuerzo para alcanzar el cumplimiento de los requisitos definidos en el ENS**.

La obligatoriedad de **actualización continua del ENS**, obligada por el Art. 42 del propio RD 3/2010 [4], se ve finalmente impulsada con un proyecto que formula una actualización global, tanto en el articulado de la norma como en los anexos, que ha sido descrita en el apartado 2.3.2 Proyecto de nuevo Real Decreto del ENS.

No obstante, dicha actualización no parece aportar argumentos para creer en un aumento relevante en cuanto al porcentaje de implantación del ENS en las entidades locales de menor tamaño con respecto a la situación actual. Las principales dificultades para la implantación son conocidas (recursos escasos, falta de concienciación en materia de seguridad de la información, falsa percepción de riesgo bajo, falta de régimen sancionador asociado al incumplimiento y demoras en el desarrollo de la Administración Electrónica, entre otras). En el proyecto de nuevo RD [6] no se incluyen modificaciones que induzcan a pensar que esta situación vaya a mejorar de manera sustancial. Concretando, por ejemplo, para las EELL de menor tamaño, en el proyecto de actualización del ENS se añaden en su art. 30 los Perfiles de cumplimiento específico buscando una mayor eficiencia en cuanto a la aplicación del ENS. Sin embargo, esta novedad no lo es tal, si tenemos en cuenta que este mecanismo ya ha venido utilizándose impulsado desde la FEMP y desde el propio CCN, que ha dispuesto de guías al respecto STIC.

En cuanto a las nuevas medidas de seguridad incluidas en el proyecto de nuevo RD, destacan por su relevancia y adaptación al desarrollo tecnológico y a las nuevas amenazas, las relativas a los servicios en la nube, navegación web, el refuerzo de la cadena de suministro (que involucra al sector privado trabajando para las AAPP), entre otras.

5 Glosario

AAPP: Administraciones Públicas
AR: análisis de riesgos
EELL: Entidades locales
ENAC: Entidad Nacional de Acreditación
ENI: Esquena Nacional de Interoperabilidad
ENS: Esquema Nacional de Seguridad
LBRL: Ley de bases de régimen local
MCE-ENS: Marco de certificación específico con el ENS
RD: Real Decreto
POC: Punto o Persona de Contacto (de Seguridad de la información)
SGBD: Sistema Gestor de Bases de Datos
STIC: Seguridad de las tecnologías de la información y la comunicación

6 Bibliografía

[1] BOE, «Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos,» junio 2007. [En línea]. Available: https://www.boe.es/eli/es/l/2007/06/22/11.

[2] BOE, «Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.,» octubre 2015. [En línea]. Available: https://www.boe.es/eli/es/l/2015/10/01/40/con.

[3] BOE, «Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.,» octubre 2015. [En línea]. Available: https://www.boe.es/eli/es/l/2015/10/01/39/con.

[4] BOE, «Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica,» Enero 2010. [En línea]. Available: https://www.boe.es/eli/es/rd/2010/01/08/3/con.

[5] BOE, «Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.,» octubre 2015. [En línea]. Available: https://www.boe.es/eli/es/rd/2015/10/23/951.

[6] Ministerio de asuntos económicos y Transformación Digital , «Proyecto de real decreto por el que se regula el Esquema Nacional de Seguridad,» junio 2021. [En línea]. Available: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/210614-PRD-ENS-TEXTO.pdf.

[7] CCN-CERT, «CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (<5.000 habitantes).,» 2020 mayo. [En línea]. Available: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4955-ccn-stic-883-guia-de-implantacion-del-ens-para-entidades-locales-anexo-i-883a.html.

[8] CCN-CERT, «CCN-STIC-803 Valoración de Sistemas en el ENS,» mayo 2020. [En línea]. Available: 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.

[9] CCN-CERT, «CCN-STIC-883 Guía de implantación del ENS para Entidades Locales,» mayo 2020. [En línea]. Available: 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.

[10] BOE, «Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014,» julio 2014. [En línea]. Available: https://www.boe.es/doue/2014/257/L00073-00114.pdf.

[11] Javier Candau, CCN, y Miguel Ángel Amutio, SGAD, «III Encuentro del ENS - Presentación CCN-CERT / SGAD,» junio 2021. [En línea]. Available: https://ens.ccn.cni.es/es/docman/documentos-publicos/iii-encuentro-ens/540-01-presentacion-ccn-cert-sgad.

[12] Ministerio de Asuntos Económicos y Transformación Digital, «Memoria del análisis de impacto normativo del proyecto de real decreto por el que se regula el esquema nacional de seguridad,» junio 2021. [En línea]. Available: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/210614-PRD-ENS-MAIN.pdf.

[13] BOE, «Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.,» enero 2021. [En línea]. Available: https://www.boe.es/eli/es/rd/2021/01/26/43.

[14] CCN-CERT, «CCN-STIC-806 Plan de Adecuación al ENS,» junio 2020. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/511-ccn-stic-806-plan-de-adecuacion-al-ens/file.html.

[15] CCN, «Marco de Certificación ENS para Entidades Locales,» [En línea]. Available: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/183-abstract-marco-de-certificacion-ens-para-entidades-locales.

[16] BOE, «Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.,» abril 2020. [En línea]. Available: https://www.boe.es/eli/es/l/1985/04/02/7/con.

[17] Instituto CIES - revisada por equipo redactor FEMP, TOMO I. Guía estratégica en seguridad para entidades locales, 2017.

[18] Ministerio de Hacienda y Administraciones Públicas, «PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[19] European Union Agency for Cybersecurity (ENISA), «Inventory of Risk Management / Risk Assessment Methods and Tools,» [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory. [Último acceso: diciembre 2021].

[20] CCN-CERT, «PILAR,» CCN, [En línea]. Available: https://pilar.ccn-cert.cni.es/. [Último acceso: diciembre 2021].

[21] CCN-CERT, «CCN-STIC 470 PILAR – Manual de usuario v7.1,» CCN, mayo 2018. [En línea]. Available: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2841-ccn-stic-470i1-pilar-manual-de-usuario-v7-1/file.html.

[22] CCN, «Sector Público Certificado,» CCN, diciembre 2021. [En línea]. Available: https://ens.ccn.cni.es/es/certificacion/sector-publico.

[23] Centro Criptológico Nacional (CCN), «800 Guías Esquema Nacional de Seguridad,» Junio 2020. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/511-ccn-stic-806-plan-de-adecuacion-al-ens/file.html.

[24] BOE, *Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local,* BOE, 1985.

7 Anexos

7.1 ANEXO I CRITERIOS DE APLICACIÓN DE MEDIDAS

Se recogen en este Anexo los criterios de selección de los controles de seguridad empleados en el apartado *3.3 Selección de las medidas de seguridad*, en aplicación del perfil de cumplimiento específico definido en la guía CCN-STIC 883A [7].

7.1.1 [ORG.1] Política de seguridad, [ORG.2] Normativa de seguridad, [ORG.3] Procedimientos de seguridad, [OP.PL.1] Análisis de riesgos

Para este conjunto de medidas, serán de aplicación los requisitos de categoría BÁSICA que, en el caso de los Ayuntamientos adheridos al Marco de Certificación de EELL, y de acuerdo con lo establecido en el *Abstract*- "**Marco de Certificación ENS para Entidades Locales**", se abordarán de manera conjunta para todos los Ayuntamientos adheridos al mismo de la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

7.1.2 [OP.EXP.7] Gestión de incidentes y [OP.EXP.9] Registro de la gestión de incidentes

Serán de aplicación los requisitos de categoría MEDIA, según los procedimientos establecidos por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente y en coordinación con ésta, relativos a la obligatoriedad de comunicación de incidentes.

7.1.2.1 [OP.EXP.8] Registro de actividad de los usuarios

Serán de aplicación los requisitos de nivel BAJO, en el sistema de información del Ayuntamiento, mientras que los relacionados con los servicios correrán por cuenta de la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

7.1.3 [OP.EXT.1] Contratación y acuerdos de nivel de servicio y [OP.EXP.2] Gestión de diaria

Serán de aplicación los requisitos de categoría MEDIA, según los procedimientos establecidos por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

7.1.4 [OP.MON.2] Sistema de métricas

Serán de aplicación los requisitos de categoría MEDIA, al ser necesarios la recopilación de los datos relativos sobre incidentes de seguridad para dar respuesta a la Encuesta INÉS (Informe Nacional sobre el Estado de la Seguridad).

7.1.5 [OP.COM.2] Protección de la confidencialidad

Serán de aplicación los requisitos de nivel MEDIO, con las siguientes particularidades:

- Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- Será recomendable que se empleen algoritmos acreditados por el Centro Criptológico Nacional.

7.1.6 [OP.COM.3] Protección de la autenticidad y la integridad

Serán de aplicación los requisitos de nivel MEDIO, con las siguientes particularidades:

- Aplicarán los requisitos de nivel BAJO íntegramente.
- Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- Será recomendable que se empleen algoritmos acreditados por el Centro Criptológico Nacional.

7.1.7 [MP.SI] Protección de los soportes de información

Para el conjunto de medidas de "[mp.si] Protección de los soportes de información", como norma general, serán de aplicación los requisitos en nivel BAJO y categoría BÁSICA, según sea de aplicación, con las siguientes particularidades:

- La medida “[mp.si.1] Etiquetado” aplicará a los dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga) cuando estos contengan información relacionada con los servicios dentro del alcance del ENS y a los documentos (formato electrónico y soporte papel) que forman parte del Sistema de Gestión de la Seguridad de la Información (SGSI).
- La medida “[mp.si.2] Criptografía”, será de aplicación con los requisitos de nivel MEDIO, en el caso de que estos vayan a ser utilizados fuera de las instalaciones.
- La medida “[mp.si.5] Borrado y destrucción”, también será de aplicación para los discos duros del equipamiento.

7.1.8 [MP.SW.2] Aceptación y puesta en servicio

Esta medida no será de aplicación al ser de aplicación al sistema de información donde residen los servicios (Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente), siendo responsabilidad de éste su aplicación.

7.1.9 [MP.INFO.4] Firma Electrónica

Serán de aplicación los requisitos en diferentes niveles para esta medida, con las siguientes particularidades:

- MEDIO: cuando se utilice firma electrónica para la actividad administrativa y esta sea necesaria para garantizar la verificación y validación de la firma electrónica.
- BAJO: cuando se utilice firma electrónica para funcionalidades distintas de la actividad administrativa.
- N.A. (no aplica): cuando no se utilice la firma electrónica en relación con los servicios que se encuentran dentro del alcance.

7.1.10 [MP.INFO.5] Sellos de tiempo

Serán de aplicación los requisitos de nivel ALTO, para aquella información que sea susceptible de ser utilizada como evidencia electrónica, siempre y cuando el servicio de sello de tiempo no sea provisto por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente, en cuyo caso la aplicación de estos requisitos será responsabilidad de esta.

7.1.11 [MP.INFO.9] Copias de seguridad (backup)

Serán de aplicación los requisitos de nivel BAJO, siempre y cuando el servicio de copias de seguridad no sea provisto por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente y no se aloje información relacionada con los servicios ENS en el sistema de información del Ayuntamiento, siendo en este caso responsabilidad del Ayuntamiento su aplicación.

7.1.12 [MP.S.1] Protección del Correo Electrónico

Serán de aplicación los requisitos de categoría BÁSICA, siempre y cuando el correo electrónico intervenga en la prestación de los servicios dentro del alcance del ENS.

7.1.13 [MP.S.2] Protección de los servicios y aplicaciones web

Esta medida no será de aplicación al ser de aplicación al sistema de información donde residen los servicios (Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente), siendo responsabilidad de éste su aplicación.