UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía de apoyo para el cumplimiento simultáneo del Esquema Nacional de Seguridad y la legislación de protección de datos

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Romero Marcos, José María

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2021/2022

Resumen

Guía para el responsable del tratamiento de datos personales y del responsable de seguridad de un organismo público o privado que tenga que cumplir el Esquema Nacional de Seguridad y el RGPD y LOPDGDD. Se guiará mediante ejemplo práctico sobre la herramienta de análisis de riesgo µPilar (CCN) y evaluación de impacto en tratamientos de datos personales EIPD (AEPD) en los casos obligados por el Reglamento General de Protección de datos y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, además de aconsejar en las posibles medidas de seguridad a aplica para dicho cumplimiento. Se diseña una Base de Datos para apoyo del registro de Actividades de Tratamiento.

Palabras clave: Esquema Nacional de Seguridad, Protección de datos, Gestión de riesgos y Evaluación de impacto en tratamientos de datos personales, Responsable de tratamiento de datos personales, RGPD, LOPDGDD.

Abstract

Guide for the personal data controller and the security officer of a public or private organization that has to accomplish with the National Security Scheme and the GDPR and LOPDGDD. It will be guided by a practical example on the µPilar risk analysis tool (CCN) and impact assessment on EIPD personal data processing (AEPD) in cases required by the General Regulation of Data Protection and the Organic Law of Data Protection and Guarantee of Digital Rights, in addition to advising on possible security measures to apply for such compliance. Database schema for recording Treatment Activities is designed.

Keywords: National Security Scheme, Data Protection, Risk Management and Impact Assessment on Personal Data Processing, Data Controller, GDPR, LOPDGDD.

Prólogo

El 4 de mayo de 2022 se publicó en el Boletín Oficial del Estado (BOE) el *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad* (ENS) para tratar de adaptarse a la situación actual con las experiencias adquiridas, o lecciones aprendidas, desde su inicio, así como a las nuevas regulaciones existentes en materias de protección de derechos personales y Ciberseguridad. Para comprender su marco jurídico y normativo hay que observar la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, cuyo artículo 12.1 señala: «Las Administraciones (AAPP) deberán garantizar que los interesados puedan relacionarse con la Administración a través de medios electrónicos…» (1) Además, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, lo especifica en su artículo 3.2: «Las AAPP se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados. » (2)

Dicho ENS (3) establece, una serie de principios y requisitos mínimos que se han de cumplir en los sistemas para el tratamiento de Servicios y Sistemas de Información, desde el momento de su concepción, estableciendo el ámbito de actuación en el Sector Público y en las Empresas del sector privado que preste un servicio en régimen de concesión, encomienda de gestión o contrato del Sector Público.

El contexto del presente Trabajo Fin de Grado es el de confeccionar una guía que ayude a Responsables de seguridad y Encargados de tratamiento de datos personales. Existe una gran cantidad de legislación y guías actuales en materia del tratamiento de Datos Personales. Se simplificarán los procesos que se han de realizar para asegurar los Derechos reconocidos y poder analizar las medidas de protección adecuadas en base a una Evaluación de Impacto, en el caso de que sea requerida. Dichas medidas de protección estarán en consonancia con lo establecido en el actual Esquema de Seguridad.

Tabla de contenidos

1. Introducción 7
2. Objetivos 11
3. Metodología. 13
4. Situación Actual. 15
5. Análisis de riesgo 17
6. Evaluación de impacto respecto a la protección de datos personales. 23
7. Medidas y garantías (controles) 29
8. Derechos de los ciudadanos. 31
9. Medidas obligatorias de todo tratamiento de datos de carácter personal. 33
10. Medidas técnicas de seguridad para el Tratamiento de Datos Personales. 37
11. Herramienta de Trazabilidad y Confidencialidad. 39

Interfaz del administrador. 40

Carla Desktop y la funcionalidad del cliente. 44

12. Herramienta para el ejercicio de los derechos. 49

Conclusiones 51

Glosario 53

Acrónimos 55

Bibliografía y referencias. 59

Anexo I. Análisis de riesgo con µPilar. 61

Anexo II. Registro de Actividades de Tratamiento del Organismo (RAT) 75

ANEXO ODS 77

1. Introducción

La protección de los datos personales es uno de los derechos fundamentales recogidos en nuestra Constitución. ¿A quién no le preocupa que todos esos datos que recogen sobre nuestra persona (físicos, genéticos…) sean usados para lo que no se nos ha asegurado que van a ser usados? Esto ha llevado a los legisladores a asegurar dichos datos mediante el marco legislativo actual, intentando minimizar los posibles incidentes, perpetrados por descuido o por intención.

Una pregunta que debemos hacernos antes de seguir es lo que se entiende por datos personales. El RGPD los define en su artículo 4 «como toda información sobre una persona física identificada o identificable» mediante algún identificador. También nos define algo que usaremos mucho, el *tratamiento*, que es «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, automatizados o no.» (4)

Una vez establecidos que son los datos y su *tratamiento*, podemos decir que el objeto de la protección de los datos personales es la de asegurarse de que dichos datos no se pierdan, alteraren o accedan sin autorización. (5) Dicha Ley Orgánica adapta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo en relación a la protección y libre circulación de datos (RGPD). En España, la Agencia que se encarga del Control que establece el RGPD es la Agencia Española de Protección de Datos (AEPD). Cuando el *tratamiento* de esos datos se produce por medios digitales, entra dentro del ámbito de actuación del ENS, siempre y cuando corresponda al Sector público y a las empresas del sector privado si la responsabilidad recae en algún organismo del Sector Público.

De lo anterior, ya hemos fijado que vamos a centrarnos en lo que cae dentro del ENS, por lo que conviene ver un poco en qué consiste ese esquema de seguridad. Se articula en tres niveles con diferentes figuras o roles de responsabilidad (1):

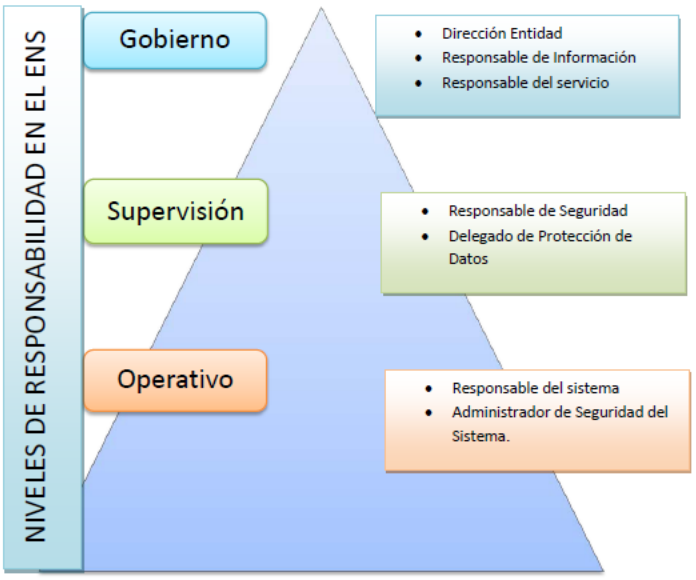
1. Nivel de gobierno: que es quien especifica y controla la adecuada prestación de servicios y el tratamiento de información.
    a. Dirección de la Entidad.
    b. Responsable de la Información. Persona que determina los niveles de seguridad de la información, según el Anexo I del ENS.
    c. Responsable del Servicio. Persona que determina los niveles de seguridad de los servicios, según el Anexo I del ENS.

2. Nivel de supervisión: En este nivel se supervisa la seguridad de la información y la ciberseguridad en la prestación de servicios y el tratamiento de la información, así como el cumplimiento de la Protección de Datos, según sea el RSEG o DPD. Estos dos roles no deberían coincidir en la misma persona, salvo carácter excepcional, según establece la AEPD.
    a. Responsable de Seguridad (RSEG). Personal que se encarga de:
        i. Satisfacer los requisitos de seguridad establecidos en la política de seguridad de la organización para la prestación de servicios y el tratamiento de la información.
        ii. Realiza o controla auditorías.
        iii. Promueve la formación y concienciación en su ámbito de responsabilidad.
        iv. Supervisa las medidas de seguridad para garantizar la seguridad del sistema.
        v. Está inmerso en la investigación de los incidentes de seguridad.

vi. Determina la categoría del Sistema de Información según valora el nivel de gobierno.

b. Delegado de Protección de Datos (DPD) le corresponden las siguientes misiones:
   i. Asesorar e informar al responsable o encargado de los tratamientos y a los empleados que de él actúen sobre las obligaciones del RGPD.
   ii. Supervisar el cumplimiento de lo dispuesto en el RGPD.
   iii. Ofrecer asesoramiento si se precisa sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
   iv. Cooperar y actuar como punto de contacto con la AEPD y con el resto de agencias autonómicas.

3. Nivel operativo: Se responsabiliza de la implantación de las medidas de seguridad del sistema, bajo supervisión del RSEG. Diferentes roles de seguridad, entre ellos
   a. Responsable del sistema (RSIS) le corresponden las misiones:
      i. Gestiona el ciclo de vida del sistema.
      ii. Criterios de uso y servicios del sistema.
      iii. Ver que las medidas de seguridad se integran en el marco de seguridad definido.
      iv. Proponer al nivel de gobierno, en caso necesario, la suspensión de la prestación de un servicio o tratamiento de información por deficiencias de seguridad.
   b. Administrador de Seguridad del Sistema (ASS), puede depender del RSEG o RSIS. Encargado de:
      i. Implementar, mantener y gestionar las medidas de seguridad del Sistema de Información, así como todo lo referente a hardware y software y la monitorización del sistema. Aplica los Procedimientos Operativos de Seguridad (POS).
      ii. Informar al RSEG o al RSIS de incidencias, anomalías, compromiso o *vulnerabilidad* de seguridad.
      iii. Colabora en la investigación y resolución de incidentes.



1 Resumen de niveles y figuras de responsabilidad en el ENS (Fuente: Propia)

De lo anterior, ya hemos obtenido una serie de figuras importantes que entran dentro de nuestro campo de actuación, RSEG, RSIS, DPD, Responsable del Servicio y Responsable de la Información. Además de las figuras indicadas, en algunos Organismos públicos se adapta a su estructura, como es el caso de las Universidades, donde existe un Comité de Seguridad TIC, que se organiza a través de la Oficina de Seguridad TIC y de los Centros de Operaciones de Ciberseguridad. (6)

2 Gobernanza en algunos Organismos. (Fuente: propia)

Como elemento esencial en una organización, desde el punto de vista de la Seguridad en el ENS, además de ser una de las medidas dentro del marco organizativo, es la definición de la Política de Seguridad. ¿Qué debe de contener? Esta debe contener, como mínimo, lo especificado en el Anexo II del ENS (3):

- Objetivos de la organización
- Marco legislativo aplicable.
- Figuras de seguridad, con sus funciones y dependencias claras.
- Si crean comités de seguridad, también su estructura, composición, funciones y dependencias.
- Directrices claras sobre documentación de seguridad.
- **Riesgos derivados de los tratamientos de datos personales.**

En este último punto, es importante señalar la consideración que da el nuevo ENS sobre el registro de actividad de tratamientos (RAT), que lo remarca en el cumplimiento del RGPD sobre la aplicación de medidas de seguridad para garantizar los principios de actuación de las AAPP con plenas garantías del derecho al honor, intimidad personal y familiar, así como a la propia imagen. (4)

Pero, ¿qué es lo que especifica el ENS respecto a ese último punto? Pues, nada más y nada menos, en su artículo 3 señala que se estará en lo dispuesto en el RGPD y en la LOPD, así como lo dispuesto por los criterios que se establezcan por la AEPD o por las agencias autonómicas de protección de datos. El responsable o encargado del tratamiento, asesorado por el DPD, realizarán un análisis de riesgo conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. (4)

Esto implica que, el análisis de riesgo efectuado al Sistema de Información al amparo del ENS, puede que no se haya cubierto específicamente la seguridad de los datos personales, y, si es así, se aplicará lo que corresponda tras la evaluación de impacto del tratamiento de Datos Personales efectuada según lo especificado en el RGPD y LOPD, así como lo especificado por el órgano de Control español AEPD en su normativa, resoluciones, circulares e instrucciones.

Y aquí es donde se sitúa este TFG.

2. Objetivos

Los objetivos del presente Trabajo son:

- Principales:
  - Generar una guía sencilla que ayude a las figuras de responsabilidad en el tratamiento de los datos personales a cumplir los principios y derechos fundamentales de los ciudadanos respectando la normativa actual, el RGPD y la LOPDGDD.
  - Guiar a los responsables sobre qué análisis de riesgos hay que realizar, no sólo lo especificado en el Esquema, sino también la Evaluación de Impacto sobre los Datos Personales (EIPD) si fuera necesaria tal y como se recoge en el RGPD y LOPDGDD.
  - Ayudar a seleccionar las medidas de seguridad que el ENS establece según la categoría del Sistema de Información.

- Secundarios:
  - Dotar de una herramienta donde se encuentren todos los formatos y modelos de escritos con el objeto de cumplir lo establecido referente a la comunicación con el ciudadano sobre sus derechos.
  - Dotar de una Base de Datos para el Registro de Actividades de Tratamiento (RAT) para el Organismo.

3. Metodología.

Para la realización del presente TFG, se ha seguido los siguientes pasos:

1. Para analizar y comprender los requerimientos de los Tratamientos de Datos Personales, en adelante tratamiento, se han realizado:
    a. Estudio del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. (4)
    b. Estudio de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (5)
    c. Estudio del ejercicio de los derechos ARCO+.
    d. Estudio del análisis de los riesgos de los tratamientos de datos personales a través de la Evaluación de Impacto establecido por la Agencia Española de Protección de datos. (7)

2. Para analizar y comprender el Esquema Nacional de Seguridad actual se han seguido lo siguientes pasos:
    a. Estudio del Esquema Nacional de Seguridad. (3)
    b. Realización del curso CCN Adaptación al ENS del Centro Criptológico Nacional (CCN).
    c. Realización del curso CCN Curso de Análisis y Gestión de Riesgos de los sistemas de información.
    d. Creación de un proyecto de Análisis de Riesgos con la herramienta µPilar del CCN (MAGERIT).
3. Confección de la Guía de apoyo para el cumplimiento simultáneo del ENS y del RGPD.
4. Desarrollo de la Herramienta de Responsable o encargado del tratamiento de Datos Personales.
5. Desarrollo del diagrama de una Base de Datos para el almacenamiento del Registro de Actividades de Tratamiento, a lo que obliga la normativa disponer y que debe ser público.

TFG

Análisis

Name	Persona	Estado	Fechas
Estudio Reglamento UE Protección de Datos 2016/697	Jose Romero	Listo	14/04/2022 hasta 9/05/2022
Estudio Ley Orgánica Protección de Datos 3/2018	Jose Romero	Listo	14/04/2022 hasta 9/05/2022
Estudio nuevo Esquema Nacional de Seguridad RD 311/2022 de 3 de mayo	Jose Romero	Listo	10/05/2022 hasta 17/05/2022
			14/04/2022 hasta 17/05/2022

Formación

Name	Persona	Estado	Fecha
Curso de Adaptación al Nuevo Esquema Nacional de Seguridad (CCN)	Jose Romero	Listo	10/05/2022 hasta 17/05/2022
			Obtención del Certificado con Aprovechamiento
Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (CCN)	Jose Romero	Listo	18/05/2022 hasta 25/05/2022
			Obtención del Certificado con Aprovechamiento
Estudio de Herramienta de Margerit microPilar (CCN)	Jose Romero	Listo	26/05/2022 hasta 12/06/2022
Estudio de Herramienta Evaluación de Impacto de Datos Personales (AEPD)	Jose Romero	Listo	04/06/2022 hasta 15/06/2022

Desarrollo

Name	Persona	Estado	Fecha
Herramienta Responsable tratamiento de datos		Listo	Junio
Guía para el responsable del sistema y responsable de tratamiento de datos		Listo	10/05/2022 hasta 04/07/2022
Base de datos para RAT		En Proceso	04/06/2022 hasta 04/07/2022

3 Planificación TFG (Fuente: Propia)

4. Situación Actual.

La mayoría de las Administraciones Públicas se encuentran inmersas en la adecuación de las medidas de seguridad actuales debido a dos circunstancias principales: La primera de ellas es que deberán adaptarse al nuevo ENS publicado en el RD 311/2022 de 3 de mayo; la segunda es que el anterior ENS no tenía en cuenta a las entidades privadas que tuvieran cedido algún tratamiento por parte de las AAPP, ni tampoco se había publicado el RGPD ni la nueva LOPDGDD en el momento de su publicación.

Por ello, existe actualmente una situación transitoria de adecuación, por un lado, al nuevo ENS y por otro al RGPD y a la LOPDGDD.

¿Quiénes deben acometer esta adaptación? Pues, como se ha señalado en la introducción, las figuras responsables de seguridad o tratamiento, también los comités de algunos organismos, además de los encargados del tratamiento de las entidades privadas que apoyan al responsable mediante contratos.

¿Cómo se actúa actualmente? Hasta ahora, se realizaba un Análisis de Riesgo, identificando los activos (esenciales o no, personal, servicios, información y reglas de negocio), pero se dejaban de lado el riesgo en los procesos de tratamiento de los datos personales y se aplicaban las medidas de seguridad según la valoración de riesgo y maduración del Sistema para la adecuación al ENS. El CCN, actualizó, en 2019, la guía CCN-STIC 801, "Esquema Nacional de seguridad. Responsabilidad y funciones", con un epígrafe especial para tener en cuenta lo especificado en el RGPD, reflejado en el último informe anual del CCN sobre el marco normativo y salvaguardias. (8) La protección en el tratamiento de datos personales es un tema que conlleva una gran responsabilidad al tener que garantizar los derechos y libertades fundamentales de los ciudadanos.

¿Quién es el responsable de la aplicación de medidas para el cumplimiento de todo lo anterior? Está claro en el RGPD y en la LOPDGDD que es el responsable del tratamiento, junto con las figuras ya comentadas. Aparece en escena el encargado de tratamiento como el responsable, dentro de una entidad privada, que lleve a cabo el tratamiento cedido por una administración pública. También el Delegado de Protección de Datos de la Entidad pública o privada, que debe ser nombrado por los responsables y comunicada al organismo de control de protección de datos según los artículos 37.7 del RGPD y 34.3 de la LOPDGDD. Este organismo de control, que obliga el RGPD, en el caso de España es la Agencia Española de Protección de Datos. Además, existen autoridades comunitarias que tienen delegadas dichas competencias. En la memoria anual de actividad de la AEPD de 2021, se puede ver que el número de Delegado de Protección de Datos tanto del sector público como privados va en aumento. (9)

En los siguientes capítulos se realizará un análisis de riesgo, se describirá una evaluación de impacto sobre datos personales, se citarán los derechos de los ciudadanos y las medidas obligatorias por normativa que se deberán aplicar a todo tratamiento de datos de carácter personal, así como un procedimiento general para el ejercicio del derecho a los ciudadanos afectados. Finalmente, se analizarán las medidas

para el cumplimiento, por un lado, del ENS y, por el otro lado, del RGPD y de la LOPDGDD.

5. Análisis de riesgo

Todo sistema de información que se encuentre dentro del ámbito de aplicación del ENS debe comenzar realizando un análisis de riesgo, con el objetivo de categorizar el sistema en BÁSICO, MEDIO o ALTO. Si, además, trata datos personales, deberá pasar un análisis de riesgo conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos personales. (4)

Si la categoría del Sistema de Información es MEDIA o ALTA, el sistema debe pasar una auditoría para la certificación de su conformidad con el ENS. En el caso de sistemas con categoría BÁSICA, bastará una autoevaluación, aunque se puede realizar una auditoría de certificación. Dichas auditorías han de pasarse cada dos años o en el momento en el que se modifique algo en el sistema que le obligue a pasarlo. Se deberá realizar una auditoría de seguridad en ese tiempo.

La determinación de la categoría del sistema se realiza en base al impacto que supondría un incidente de seguridad sobre la información o sobre los servicios. El análisis se realiza sobre las dimensiones de seguridad: [C] *Confidencialidad*; [I] *Integridad*; [T] *Trazabilidad*; [A] *Autenticidad*; [D] *Disponibilidad*.

Se va a analizar a continuación los pasos para realizar dicho análisis de riesgo.

1. Lo primero es identificar los activos del sistema. Lo normal es identificar aquéllos que sean esenciales para el sistema para no olvidarlos. Se analizarán los niveles de seguridad por cada dimensión de seguridad.
    - Nivel de seguridad BAJO con respecto a alguna dimensión: *Perjuicio* al activo en la dimensión considerada limitado.
    - Nivel de seguridad MEDIO con respecto a alguna dimensión: *Perjuicio* grave sobre las funciones de la organización, activos o individuos afectados.
    - Nivel de seguridad ALTO con respecto a alguna dimensión: *Perjuicio* muy grave sobre funciones, activos o individuos.

    Cuando el sistema de información disponga de varios activos de información, servicios, el nivel de seguridad para cada dimensión será el más elevado para cada servicio o información.

2. El siguiente paso es determinar la categoría del sistema, que pueden ser tres como ya se ha comentado: ALTA, MEDIA, BÁSICA.

- ALTA: Si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.
- MEDIA: Si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO y ninguna un nivel superior.
- BÁSICA: Si todas sus dimensiones de seguridad tienen el nivel de seguridad BAJO y ninguna un nivel superior.

3. Una vez hallado el nivel de riesgo por dimensiones y la categoría de seguridad del sistema, ya se está en disposición de utilizar la tabla del anexo II del RD 311/2022, de 3 de mayo (3), donde se especifican las medidas de seguridad con sus refuerzos que se han de aplicar para cumplir con el ENS. Dichas medidas se engloban en los tres marcos, Organizativo, Operativa y medidas de protección. En azul, vemos como cada medida de seguridad por dimensiones, se debe ver el nivel de esa dimensión para ver si se aplica o no y sus posibles refuerzos. En círculo verde vemos las que se aplican según la categoría de seguridad del sistema de información.

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

4 Medidas de Seguridad o salvaguardia (Fuente: RD 311/2022)

Se marca en rojo lo que más interesa a efectos de protección de datos, que es la medida de protección mp.info.1, donde se especifica que los requisitos son:

Cuando el sistema trate datos personales, el RSEG los recogerá del responsable o encargado de tratamiento, contando con el asesoramiento del DPD, que sean necesarios implementar en los sistemas según la naturaleza, alcance, contexto y fines de esos datos, así como los riesgos para los derechos y libertades especificados en artículos 24 y 32 del RGPD. También se deberá o no pasar la Evaluación de Impacto relativa a la protección de Datos Personales según el artículo 35 del RGPD. (4)

Las medidas técnicas y organizativas que especifica el artículo 32 del RGPD (4), aplicables según lo anterior son:

a) la *seudonimización* y el cifrado de datos personales;

b) la capacidad de garantizar la *confidencialidad*, *integridad*, *disponibilidad* y permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la *disponibilidad* y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

El informe de riesgos se completará con la aceptación de los riesgos residuales del sistema, que podrán ser aceptados formalmente por los Responsables de los Servicios y por los Responsables de la Información.

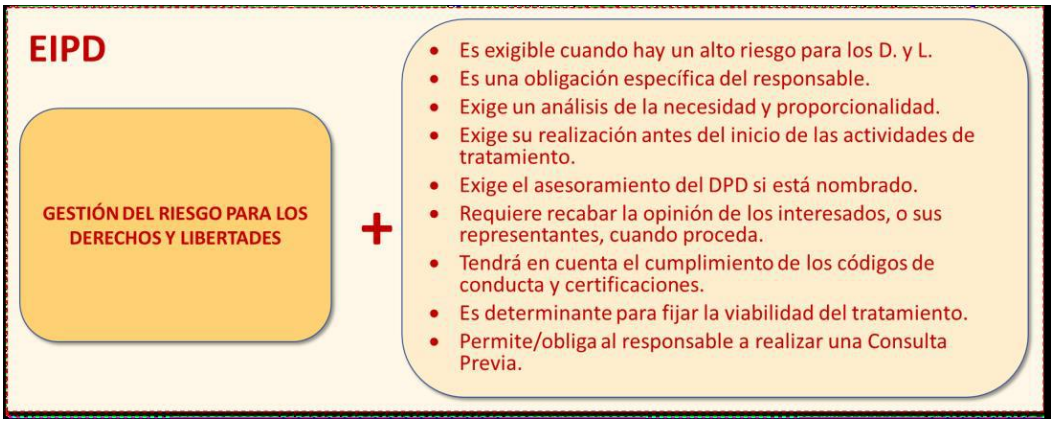
En el Anexo I se utiliza la Herramienta μPilar con metodología MAGERIT del CCN. Dicha herramienta puede ser adquirida gratuitamente y descargada desde la página del CCN. Necesita de una licencia que puede ser solicitada directamente al Centro. En este ejemplo se ha usado una licencia prestada de un Organismo para este TFG. Con dicha herramienta, el análisis es más guiado y sencillo que ir haciéndolo de forma manual. Se puede elegir el marco de análisis de riesgo para adecuación al ENS.

Junto a esta guía se puede encontrar un proyecto de análisis de riesgo con dicha herramienta como ejemplo.

6. Evaluación de impacto respecto a la protección de datos personales.

El RGPD lo define como «un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos» (4). Por lo tanto es un proceso que dura todo el ciclo de vida del tratamiento de datos personales, con revisión continuada.

En la tabla siguiente se pueden ver sus características:



5 Evaluación de Impacto Protección de Datos (Fuente: AEPD)

Una de las preguntas más importantes a la hora de iniciar o no la EIPD es ¿es obligatorio? Para ello, hay que analizar algunos artículos del RPGD y de la LOPDGDD. Esto es lo que se puede extraer:

6 Obligación de realizar EIPD (Fuente: Propia)

Una vez vista la obligación de realizarla, los pasos para este proceso EIPD son (7):

- El primer paso es identificar los factores de riesgo o las *amenazas* para D y L. La AEPD, en todas sus herramientas en los que identifica los factores de riesgo, las agrupa en categorías. Dentro de cada una de ellas les asigna un riesgo mínimo identificado.

Operaciones relacionadas con los fines de tratamiento	Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.
Tipos de datos utilizados	Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.
Extensión y alcance del tratamiento	Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.
Categorías de interesados	Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.
Factores técnicos del tratamiento	Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.
Recogida y generación de datos	Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.
Efectos colaterales del tratamiento	Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Categoría del responsable/encargado	Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
Comunicaciones de datos	Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.
Brechas de seguridad	Factores de riesgo que se derivan de la posible materialización de brechas de seguridad sobre los datos personales.

7 Categorías de factores de riesgo. (Fuente: AEPD)

Dentro de todas esas categorías, se incluyen una serie de factores de riesgos, a los que se corresponde un determinado nivel de riesgo mínimo, que puede ser Bajo, Medio Alto o muy Alto. Se pueden observar en el Capítulo VI de Identificación y análisis de FR,s. (7)

- Analizar su impacto y probabilidad. Es tarea del responsable del tratamiento determinar su impacto en función del daño que se pueda ocasionar a corto, medio y largo plazo sobre los interesados en el ámbito de D y L. La propuesta que hace el organismo de control es en función de impacto y probabilidad para determinar su nivel de riesgo.
-

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

8 Tabla Probabilidad/impacto para determinar riesgo. (Fuente: AEPD)

La AEPD hace unas consideraciones sobre los valores de impacto y de probabilidad usados en las siguientes tablas:

Nivel de impacto	Descripción
Muy significativo (irreversible)	Afecta al ejercicio de D y L.
	Y/o afectan a categorías especiales de datos o temas de datos penales.
	Y/o perjuicio social grave (por ejemplo, discriminación).
	Y/o afecta a interesados que se encuentran en especial vulnerabilidad, por ejemplo, niños.
	Y/o provoca pérdidas materiales o morales considerables.
Significativo (reversible)	Todos los casos anteriores.
	Y/o pérdida de control sobre sus propios datos personales.
	Y/o se produce o puede producirse usurpación de la identidad de la persona.
	Y/o pueden producirse pérdidas financieras graves.
	Y/o pérdida de *confidencialidad* de datos
Limitado (irreversible)	Pérdida limitada del control de algún dato personal que no sea de categoría especial.
	Y/o pérdidas financieras irrelevantes.
	Y/o pérdida de *confidencialidad* de datos que, sin ser categoría especial, están sujetos al secreto profesional.
Muy limitado (reversible)	Todas las enumeradas en limitado.

9 Consideraciones sobre nivel de impacto. (Fuente: Inspirado en AEPD)

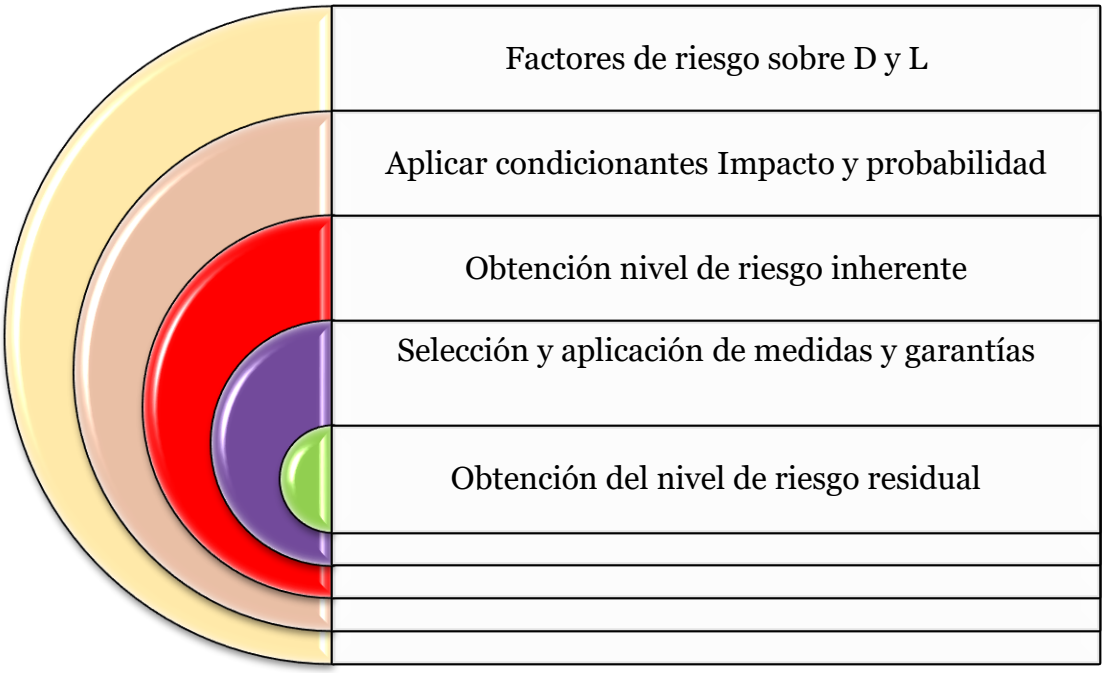
Probabilidad de ocurrencia	Condiciones
Muy Alta	Su probabilidad está fijada por tecnología o normativa. Su ocurrencia no tiene nada que ver con la probabilidad.
	Y/o ocurrencia en distintos organismos en el último año.
	Y/o ocurrencia en el último año en el mismo organismo.
	Y/o auditorías reflejan altas *vulnerabilidades* relacionadas con dicho riesgo.
Alta	Ocurrencia del factor de riesgo en algún organismo en el último año.
	Y/o análisis que fijan esa alta probabilidad de ocurrencia.
	Y/o auditorías reflejan *vulnerabilidades,* en ningún caso altas, relacionadas con dicho riesgo.
	Y/o uso de tecnologías o procedimientos inmaduros, sin acreditar.
Baja	Si hay ocurrencia en algún organismo en los últimos diez años.
Improbable	Si no ha habido ocurrencia del factor de riesgo.

10 Consideraciones sobre probabilidad de ocurrencia. (Fuente: Inspirado en AEPD)

- Evaluar el nivel de riesgo del tratamiento: Para evaluarlo, lo primero que se ha de hacer es evaluar qué impacto se obtendría de producirse una brecha de datos personales, analizando cada una de las dimensiones de seguridad del ENS ([C] *Confidencialidad*; [I] *Integridad*; [T] *Trazabilidad*; [A] *Autenticidad*; [D] *Disponibilidad*) y las siguientes nuevas dimensiones [R] *Resiliencia*, [F] Fallos en las garantías de *privacidad* y [E] Errores en las operaciones técnicas.

Dimensión: C/D/I/T/A/R/F/E					
Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

11 Tabla Probabilidad/impacto para la obtención del riesgo. (Fuente: AEPD)



12 Evaluación riesgo Inherente y Residual. (Fuente: Propia).

La forma más habitual de llegar al nivel de riesgo inherente es usando una aproximación simplificada. Se dispone de los factores de riesgo con el nivel de riesgo identificado. Se le da a cada Factor de riesgo (FR) un valor de nivel con la siguiente valoración:

- Bajo: 0.2
- Medio: 0,5
- Alto: 0,7
- Muy Alto: 0,9

Y se calcularía de la siguiente forma, sean FR1…FRn los riesgos identificados y NR1…NRn los niveles de riesgo correspondientes, el Nivel de Riesgo del tratamiento (NRT) será el siguiente:

NRTa = (NR1 + NR2) – (NR1 * NR2)

NRTb = (NRTa + NR3) – (NRTa * NR3)

…

NRT= (NRTx + NRn) – (NRTx * NRn)

De esta forma se obtendrá el **Nivel de Riesgo del Tratamiento** se puede transformar en alguno de los cuatro valores (bajo, medio, alto y muy alto) por la siguiente correspondencia:

Bajo: < 0,4 Medio: >=0,4 y < 0,6 Alto: >=06 y <0,9 Muy Alto: >=0,9

Tras este análisis, se aplicarán una serie de medidas y garantías para minimizar el nivel de riesgo a uno residual que pueda ser asumido por la organización. Se verá en el siguiente capítulo.

Para la realización de esta EIPD existe una herramienta[1] proporcionada por la AEPD que nos permite llegar al Nivel de Riesgo del Tratamiento.

13 Herramienta Evalúa Riesgo de la AEPD (Fuente: Propia)

[1] https://www.aepd.es/es/herramienta/EvaluaRiesgo_RGPD.zip

7. Medidas y garantías (controles)

En este capítulo se mostrarán unos ejemplos de medidas y garantías, comúnmente denominadas controles, para afrontar los riesgos. Al estar incluidos dentro del ENS, la mayor parte de ellas ya son implementadas por el cumplimiento de dicho Esquema. El responsable o encargado del tratamiento ha de afrontar el riesgo. Es únicamente una ayuda con unas medidas ejemplo dividas en cuatro dimensiones (7):

- **Concepto y diseño del tratamiento**. Actúan en la definición de la naturaleza, ámbito, contexto o fines del tratamiento. Como ejemplo de estas medidas podría ser:
    - Reorganizar fases del tratamiento (naturaleza)
    - Supervisión humana de las decisiones automatizadas (naturaleza)
    - Que el tratamiento se oriente a un menor número de personas (ámbito).
    - Casos de uso concretos con ámbitos disjuntos (ámbito).
    - Delimitar contextos económicos o sociales (contexto)
    - Limitar los fines del tratamiento (fines)
- **Gobernanza y políticas de protección de datos**. No puede faltar dentro de la organización.
    - Roles, sus responsabilidades y los recursos necesarios para la PD.
    - El DPD debe encontrarse en todos los procedimientos de toma de decisiones y en la definición de todos los tratamientos.
    - La PD se encontrará tanto en procedimientos en local, como en remoto o teletrabajando.
    - Todo interesado debe poder comunicarse con el organismo para la ejecución de sus D y L y su *privacidad*.
    - Establecimiento de seminarios o charlas de concienciación o formación del personal que se encuentra inmerso en nuevos tratamientos.
- **Protección de datos desde el diseño**. Para la AEPD es muy importante este punto y ha desarrollado una amplia guía de *privacidad* desde el diseño. (10) En este punto, interesa señalar cómo las estrategias que se emplean se dividen en dos aspectos importantes:
    - En privacidad de datos, donde se intentará: minimizar el número de DP que se usen; ocultar aquéllos que no necesiten ser expuestos; separarlos en conjuntos disjuntos y abstraer dichos datos, evitando bajar al detalle.
    - Privacidad en procesos., donde se intentará: informar al máximo sobre el mismo; hacer que los individuos dispongan de pleno control de sus DP; cumplir escrupulosamente la política del organismo y demostrar que en realidad se han cumplido dichas políticas.

En cuanto a los controles que se utilizan en dichas estrategias, se nombrarán las más importantes:

- En cuanto a la privacidad de los datos: La *Anonimización* y la *seudonimización* para minimizar y ocultar los DP, además del *cifrado homomórfico* y *modelos de conocimiento cero (ZKP)* para ocultar y limitar lo que se muestra. Se usará la separación física y lógica de conjuntos de datos. Y por lo que respecta a la abstracción de datos, uno de los controles más usados es el uso de la K-anonimidad y la *privacidad* diferencial
- Respecto a los procesos, se deben informar sobre el rendimiento, los límites, las consecuencias y el análisis de riesgo del tratamiento. Además, de la realización de auditorías y registro y control documental.

- **Seguridad en el tratamiento**. Al estar sometidos al ENS, se puede realizar una correspondencia en función del riesgo entre una y otra, es decir, de la EIP y del ENS. Como ya se ha comentado al tratar el análisis de riesgo desde ENS, prevalece el nivel de riesgo obtenido en la EIPD en el trato de datos personales a la hora de calcular el riego del tratamiento.

Nivel de riego EIPD	Categoría de ENS
Muy alto	Alto
Alto	Alto
Medio	Medio
Bajo	Bajo

14 Correspondencia entre nivel de riesgo EIPD y ENS (Fuente: AEPD)

8. Derechos de los ciudadanos.

Los derechos reconocidos a los ciudadanos por el RGPD y la LOPDGDD son los siguientes (4) (5):

a. De acceso. El interesado puede obtener la confirmación de si se están o no tratando datos personales suyos y obtener una copia de los mismos.
b. De rectificación. Posibilidad que tiene el interesado de obtener la rectificación de los datos que no sean correctos para garantizar su exactitud.
c. A la cancelación o supresión u olvido. Posibilidad de eliminar sus datos personales en determinadas circunstancias.
d. A la limitación del tratamiento. Posibilidad de que no se apliquen a sus datos personales las operaciones del tratamiento.
e. A la portabilidad. Posibilidad de recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica para transmitirlos a otros responsables del tratamiento.
f. De oposición. Posibilidad de solicitar que finalice el tratamiento de sus datos personales en determinadas circunstancias.

Para garantizar poder ejercer estos derechos, se debe establecer un procedimiento y unas figuras que deberán garantizar ese procedimiento. En el capítulo siguiente se tratará de especificar las medidas obligatorias que se deberán tener en cuenta al diseñar dicho procedimiento general.

9. Medidas obligatorias de todo tratamiento de datos de carácter personal.

Se incluyen las siguientes medidas generales:

a. **Licitud del tratamiento**. Tiene que ver con las causas contempladas en el artículo 6.1 del RGPD: El consentimiento; la ejecución de un contrato; una obligación legal o una competencia pública. (4)El consentimiento es un caso que la AEPD ha dejado como residual para la Administración.

   Si los datos tienen que ver con categorías especiales según el artículo 9.1 del RGPD, además se ha de cumplir alguno de los requisitos establecidos en el 9.2. (4)

b. **Registro de Actividades de Tratamiento**. Cada responsable deberá llevar un registro de las actividades de tratamiento bajo su responsabilidad, que contendrá los datos especificados en el artículo 30 del RGPD (4):
   - Nombre y datos del responsable del tratamiento y del DPD.
   - Fines del tratamiento.
   - Categorías de interesados y de los datos personales.
   - Si existe transferencia de datos personales a un tercer país u organización internacional.
   - Plazos para la supresión por categorías de datos.
   - Descripción general de medidas técnicas y organizativas de seguridad.

c. **Notificación de violaciones de seguridad a la autoridad de control y al interesado**. El responsable del tratamiento tiene un plazo de 72 horas para comunicarlo a la Autoridad de Control competente, a no ser que no haya ningún riesgo para los derechos y libertades.
d. **Designación del Delegado de Protección de Datos**. Deberá tener capacitación técnica, recursos y competencia internas suficientes según el artículo 37 a 39 del RGPD. (4)
e. **Derecho de información a los afectados en la recogida de datos**. En todos los formularios de entrada de datos de los interesados deberá contener cláusulas informativas según establece el artículo 13 del RGPD. (4)
f. **Derechos ARCO+ (Los especificados en el capítulo anterior)**. Esto es lo que todo responsable de tratamiento debe implementar para que el procedimiento de los tramitadores sea eficiente en la gestión de las solicitudes de derechos. Aquí se enmarca la herramienta de modelos que se desarrolla en el presente TFG.
g. **Cesiones de datos**. Todo aquello que se realice dentro del organismo no se considera cesión de datos.

h. **Proveedores de servicio con acceso a datos**. Este punto se debe tener muy en cuenta en los contratos públicos de servicios, ya que el Responsable del Tratamiento ha de valorar si los encargados ofrecen garantías suficientes y regularlo mediante contrato o acto jurídico vinculante. Dicho contrato o acto jurídico deberá llevar los siguientes datos como anexo para el encargado de tratamiento de datos de carácter personal en el que se obligará a:
    - Utilizar los datos únicamente para la finalidad del tratamiento.
    - Informar inmediatamente de cualquier infracción del RGPD o normativa de protección de datos.
    - Un Registro de todas las categorías de Actividades de Tratamiento.
    - No comunicar datos a terceros a no ser que exista autorización del Organismo en supuestos legales.
    - Especificar específicamente la subcontratación con Empresas y condiciones sobre tratamiento.
    - Deber de secreto en todos los datos que haya tenido acceso por el cargo.
    - Deber de *confidencialidad* de todas las personas autorizadas.
    - Formación a todas las personas autorizadas.
    - Colaborar con el Responsable en las comunicaciones sobre el ejercicio de los derechos de los interesados.
    - Si realiza alguna recogida de datos, facilitar la información relativa a los tratamientos que va a realizar consensuada con el responsable.
    - En la violación de seguridad de datos, notificar al Organismo, con posibles consecuencias y medidas adoptadas o propuestas.
    - Colaborar con el responsable en EIPD, cuando proceda, en consultas previas a la autoridad de control, y dar información que demuestre el cumplimiento de sus obligaciones.
    - Sobre las medidas de seguridad establecidas en el ENS y en los pliegos del contrato y anexos.
    - Disponer de DPD cuando así se exija según el RGPD.
    - Cuando finalice, se devolverá o destruirá la información según se especifique.
    -

i. **Proveedores de servicios sin acceso a datos**. Se deberá incluir un compromiso de *confidencialidad* que garantice el respeto a la *confidencialidad* de los datos que pudieran llegar a acceder de forma accidental según se especifica en el apartado anterior respecto a confidencialidad.

j. **Limitación del plazo de conservación**. En el artículo 5.1 e) del RGPD establece, como norma general, que serán eliminados aquellos datos que dejen de ser necesarios para los fines para los que fueron recabados. Esto no siempre es así, ya que puede haber normativa que exige un plazo de supresión determinado o que no se eliminen. Por ejemplo, la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, dependerá de su valor histórico.

k. **Deber de *confidencialidad***. Firma de compromisos de *confidencialidad* a todo el personal que intervenga en cualquier fase de tratamiento de datos de carácter personal, aún después de finalizar la relación del obligado con el responsable.
l. **Análisis de riesgos**. El artículo 32 y 76 del RGPD especifican a necesidad de realizar, para cada tratamiento, un análisis de riesgos para determinar las medidas de seguridad adecuadas y necesarias a aplicar. (4)
m. **Evaluación de impacto de protección de datos (EIPD) y consulta previa.** Si el tratamiento puede derivar en un alto riesgo para los derechos y libertades de las personas físicas, se llevará a cabo una EIPD. Si entraña un alto riesgo, en ningún caso se puede proceder a llevar a cabo el tratamiento y, el responsable deberá establecer las medidas necesarias para mitigar ese riesgo **o consultar a la AEPD** a través de su DPD si se puede o no llevar a cabo el tratamiento.
n. **Regulación de las transferencias internacionales de datos.** Cuando sean a países fuera del Espacio Económico Europeo (UE, Liechtenstein, Islandia y Noruega), hay que aplicar los artículos 44 a 49 del RGPD. (4)
o. **Inclusión de textos legales obligatorios en páginas WEB.** Normalmente es el órgano de Control (AEPD) quien fija los avisos legales, políticas de *privacidad* y cookies, etc.
p. **Responsable de Seguridad.** Se deben designar uno o varios responsables que pueden serlo de varios tratamientos.

10. Medidas técnicas de seguridad para el Tratamiento de Datos Personales.

Se deberán seguir las medidas de protección previstas en el ENS en su anexo II. Por parte del CCN se pueden autorizar cumplimientos específicos dentro de sus guías para entidades o sectores.

En este apartado, se va a intentar dar unas posibles medidas generales a implantar en tratamientos con datos personales.

a) Fijar responsabilidades al personal que trata datos de carácter personal. Este punto es el responsable del tratamiento el que ha de fijar las obligaciones y responsabilidades.
b) Formación y concienciación para dicho personal.
c) Gestión y registro de *incidentes*. Existe una solución que se ofrece por el CCN para este punto **Gloria**, es una plataforma para la gestión de *incidentes* y *amenazas* de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM (Security Information and Event Management), va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes. También se dispone de la solución **Lucía**, el organismo podrá gestionar tres tipos de ciberincidentes: Los *incidentes* propios del Organismo; Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA) y Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).
d) Control de acceso físico a las instalaciones. El ENS lo lleva implementado.
e) Sistemas de videovigilancia, también contemplados y ya hemos visto que además son objeto de control como dato de carácter personal.
f) Ficheros temporales o copias de ficheros han de llevar también unas medidas de seguridad estrictas para garantizar la *confidencialidad*, *integridad* y *trazabilidad*. Como veremos en el capítulo de Herramienta para *trazabilidad* y *confidencialidad*, **CARLA** es una solución muy atractiva para estos atributos.
g) Transferencia de información a terceros. Importante la solución anteriormente citada Carla, que se verá en mayor detalle.
h) Bloqueo de equipos informáticos. Introducidas, como las anteriores, dentro de la política del sistema.
i) Acceso a datos a través de redes de comunicación. **EMMA** es una solución que recomienda el CCN-CERT como herramienta para conseguir Vigilancia sobre la red.
j) Derechos de acceso. Con el objeto de conseguir los principios mínimos de mínimo privilegio, necesidad de conocer y capacidad de autorizar. La

implementación de procedimientos de revocación de accesos a empleados es muy importante.

k) Protección de equipos portátiles fuera de los locales del responsable. Las medidas más importantes son:
    a. Inventario
    b. Gestión de *incidentes*
    c. Criptografía.
    d. Custodia
    e. Transporte
    f. Borrado y destrucción.

Y, en cuestión de datos de carácter personal, resaltar siempre la importancia de la *trazabilidad*. Es una de las características de seguridad que nos permite ver quién y dónde han tenido acceso a los datos. Es por este motivo que se dedica un capítulo a hablar de la solución más reciente del CCN-CERT, Carla, con la que podemos compartir incluso en internet, ya que sólo tienen acceso las personas que se les otorgue autorización, y garantiza la *confidencialidad* al ir cifrado.

11. Herramienta de Trazabilidad y Confidencialidad.

se 

CCN-CERT dispone de una solución que permite a las AAPP y organizaciones proteger sus documentos, incluso cuando han sido enviados fuera del control de las propias entidades. Esta solución es CARLA. Con ello evitan fugas de información por acciones involuntarias o no del propio personal, al poder revocar los accesos previamente autorizados y acceso a ficheros protegidos.

Una vez implementada la solución aporta las siguientes ventajas:

- Protección de la información donde esté, evitando fugas de datos.
- Facilita la colaboración segura con un tercero, al auditar y controlar los accesos.
- Control y visibilidad de los mismos y de sus accesos
- Ayuda a cumplir normativa de protección de datos (*trazabilidad* y *confidencialidad*).
- Protege frente a posibles brechas de seguridad que se produzcan en el sistema, al ir cifrado.
- Sencillez de uso para los usuarios y administradores.

Existen dos modalidades de instalación de la solución:

Carla: pensada para un servicio limitado a un subconjunto de usuarios de la organización con funcionalidades básicas, también denominada Carla Base u on-premise.

Carla Global: diseñada para despliegue en toda la organización e incluye todos los módulos opcionales.

En la primera opción, el servidor validador se encuentra en la Organización, y si se comparte información fuera del organismo, se deberán abrir puertos para que terceros puedan llegar a validarse y adquirir así los acceso al fichero compartido. En la segunda, la validación puede ser realizada directamente contra servidores en el CCN.

Su funcionamiento es muy sencillo, con esta imagen del CCN-CERT donde se explica la herramienta, se puede ver lo fácil que es.

15 Comportamiento de la solución. (Fuente: CCN)

Esta solución se encuentra disponible a través de partners certificados por CCN. Su precio dependerá de los servicios de nivel 2. El nivel 2 depende del número de usuarios y opciones contratadas. En la actualidad hay cuatro, tabla obtenida de https://www.ccn-cert.cni.es/soluciones-seguridad/carla.html:

Nombre	Razón social	Web	Estado de certificación
CSA	Centro Regional de Servicios Avanzados, S.A.	www.csa.es	CERTIFICADA (01/02/2021)
EntelgyInnotec Security	InnoTec System, S.L.U.	Innotec.security	CERTIFICADA (01/02/2021)
Grupo ITE	Integración Tecnológica Empresarial, S.L.	www.ite-es.com	CERTIFICADA (01/02/2022)
Sidertia	Sidertia Solutions S.L.	sidertia.com	CERTIFICADA (01/02/2021)

16 Partners certificados. (Fuente: CCN)

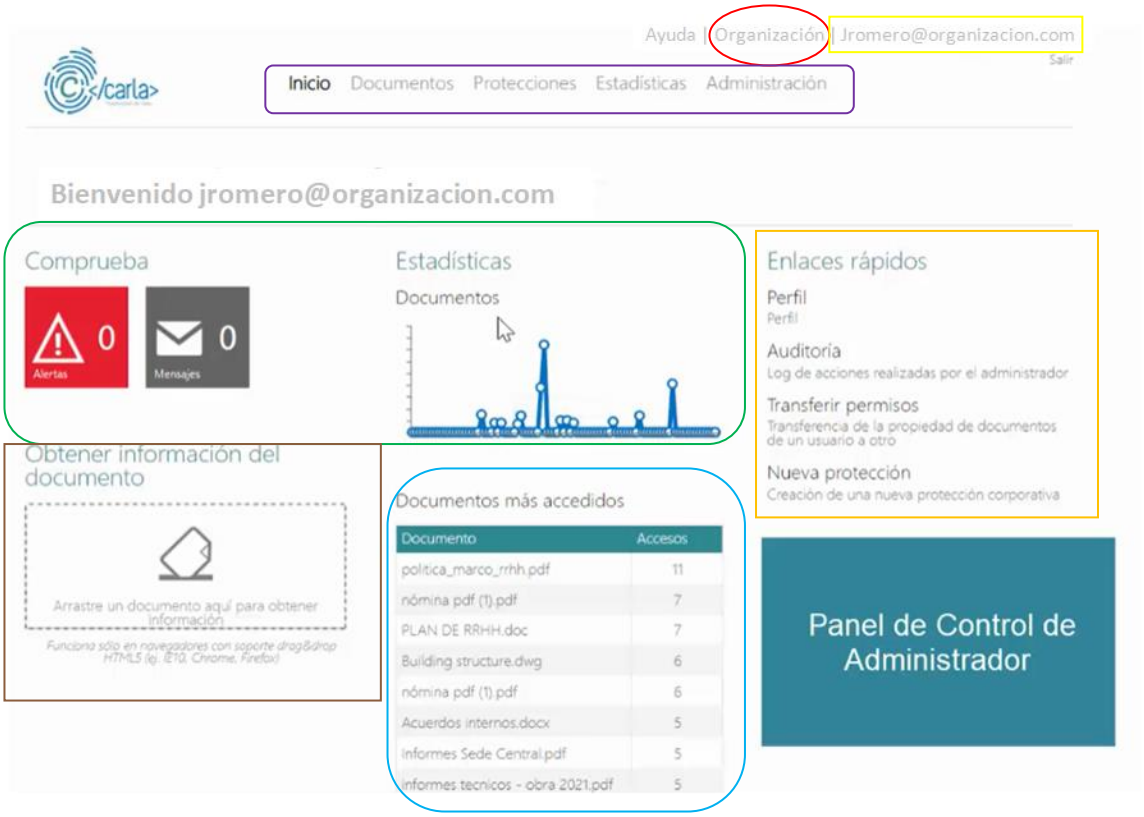
Interfaz del administrador.

A continuación, se explicará en detalle la forma en la que se protegen documentos mediante la opción on-premise dentro de la misma organización.

En la organización hay que configurar un servidor validador con Windows Server, en donde se instala el servidor de validación SEALPATH. En él, se tendrá acceso a la consola de la herramienta administrador. En las máquinas clientes de la organización se instalará la aplicación Carla Desktop, donde los clientes podrán proteger sus archivos o carpetas, bien en base a una política definida por el administrador, bien por una política ad-hoc creada por el cliente o sin política, en base a una configuración para un solo uso. En los usuarios externos, necesitarán instalar Carla live para validarse con las credenciales con las que se registren.

Como se verá en el menú de administración, los usuarios pueden ser locales a la aplicación, creados en la interfaz, grupos o usuarios del dominio activo (AD/LDAP) o externos a la organización.

Se muestra la interfaz de administrador, que se accede por web.



17 Captura pantalla principal interfaz de administrador.

En la captura anterior se muestra, en rojo, el nombre de la organización, en este caso Organización. En amarillo, se puede ver el usuario administrador, en púrpura, el menú principal del interfaz, en verde unas estadísticas de alertas sobre documentos, en marrón, se puede arrastrar un documento para obtener la información de su protección, y poder saber con qué política y que usuario lo protegió, accesos, etc. También, en azul, una tabla con los documentos más accedidos en la organización, así como, en naranja, unos enlaces rápidos a auditorías realizadas sobre los administradores de la solución Carla. Esta auditoría se puede exportar a un fichero csv para poderse analizar.

En la opción de menú Documentos, se pueden ver los documentos ordenados por acceso de usuario, eligiendo en opciones por su acceso de usuarios tanto externo como interno de la organización, por protección, según su política de protección y las alertas. Todo ello con la posibilidad de exportación a fichero csv.

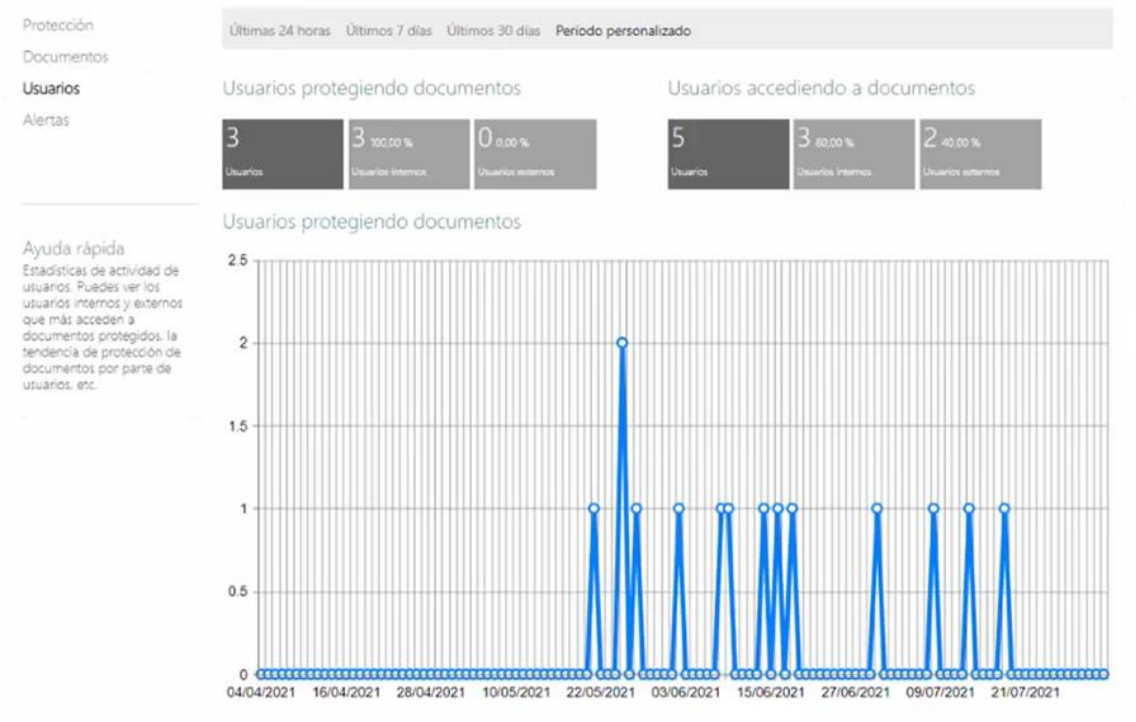
18 Menú Documento del interfaz de administrador.

En la opción de menú protección, se tiene acceso a todas las políticas de protección creadas por el administrador, de forma corporativa, y a las creadas por los usuarios particulares de la aplicación. Esto es muy importante, ya que el administrador central de la aplicación puede modificar la política, atributos de seguridad, usuarios que tengan acceso, etc.

Toda política corporativa que se cree, se deberá dar acceso a los usuarios que finalmente la utilicen.

19 Menú Protecciones del interfaz del administrador.

El menú Estadísticas, nos dará la información gráfica y tabular sobre protección, documento, usuario y alertas.



20 Menú Estadísticas del interfaz del administrador.

El menú Administración dispone de las herramientas más potentes.

21 Menú Administración del interfaz del administrador.

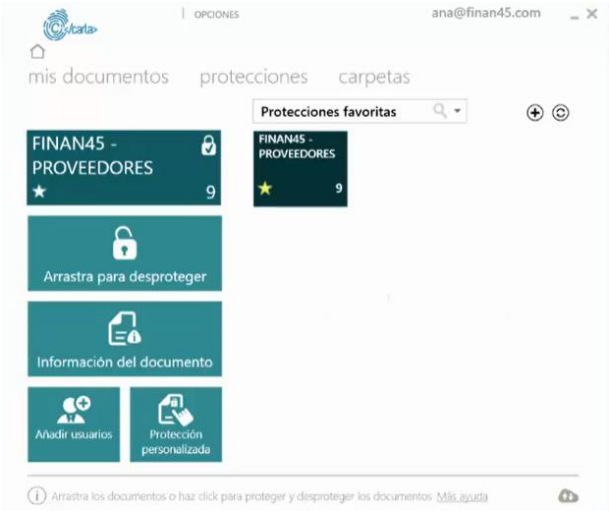
La opción de transferir permisos, permite al administrador, que, si algún usuario ha dejado la organización, transferir los documentos protegidos por las políticas seleccionadas, bien sean corporativas o de usuario, a otro usuario de la organización. Con la opción bloquear acceso, bloquea inmediatamente los documentos que se nos pidan. En la Auditoría, se pueden ver todas las acciones llevadas a cabo por los administradores, y pueden ser descargados a un fichero csv. Y una opción muy importante es la de superusuario, ya que se puede crear un usuario, que únicamente funcionará un tiempo, si hemos perdido todas las opciones de control de la herramienta. Esto nos permitirá restaurar la organización a un estado operativo y salir de la emergencia.

Como se puede ver es una solución muy importante para *trazabilidad* de datos y *disponibilidad*. En el siguiente apartado, se verá cómo funciona la herramienta Carla Desktop para proteger documentos, carpetas, crear políticas, proteger adjuntos que se envía por email, etc.

Carla Desktop y la funcionalidad del cliente.

No se ha podido tener acceso a la funcionalidad cliente, por lo que todo lo que se muestre en este apartado se ha obtenido de formación a través de la plataforma VANESSA del CCN.

La pantalla principal de la aplicación será de esta forma:



22 Pantalla principal de CARLA DESKTOP (Fuente: VANESSA-CCN)

Al ejecutar la aplicación Carla Desktop, el cliente puede interactuar con las políticas creadas de forma corporativa y compartida por el administrador, o, en su defecto, crear nuevas políticas que, a su vez, puede compartir con otros usuarios.

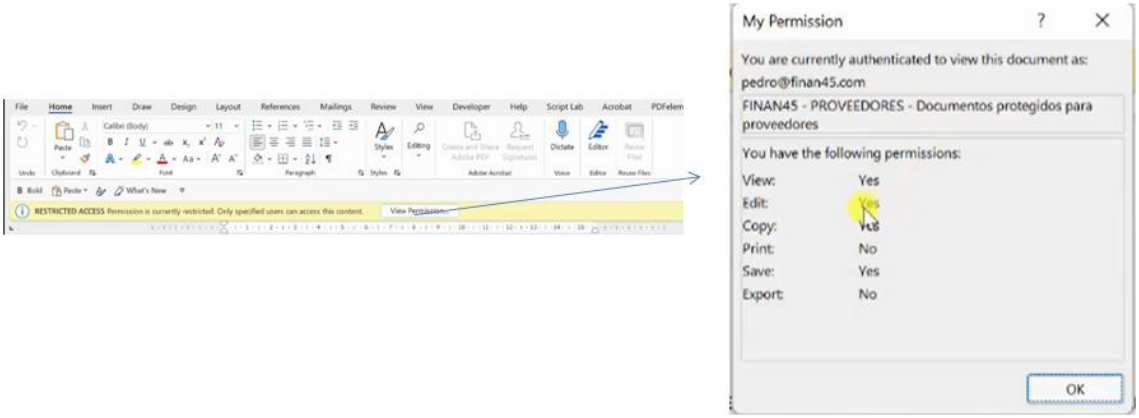
En la captura 24 se puede apreciar una política que le ha sido compartido al usuario ana@finan45.com. La forma de aplicarla a un fichero es tan sencillo como arrástralo sobre la plantilla FINAN45-PROVEEDORES. A partir de ese momento la carpeta o fichero estará protegido siguiendo las especificaciones dadas por la plantilla respecto a: usuarios permitidos con los permisos para cada uno, la fecha de expiración del documento desde la que no se podrá acceder, la marca de agua tanto a página como a imágenes del documento.

A partir de ese momento, aparecerá un icono sobre el fichero protegido. En la figura siguiente se pueden ver dos ficheros con dicha protección, un fichero docx y un PDF.

23 Ficheros protegidos por CARLA

Los ficheros protegidos por CARLA dentro de la organización se pueden abrir con las herramientas habituales, Word, Acrobat Reader.

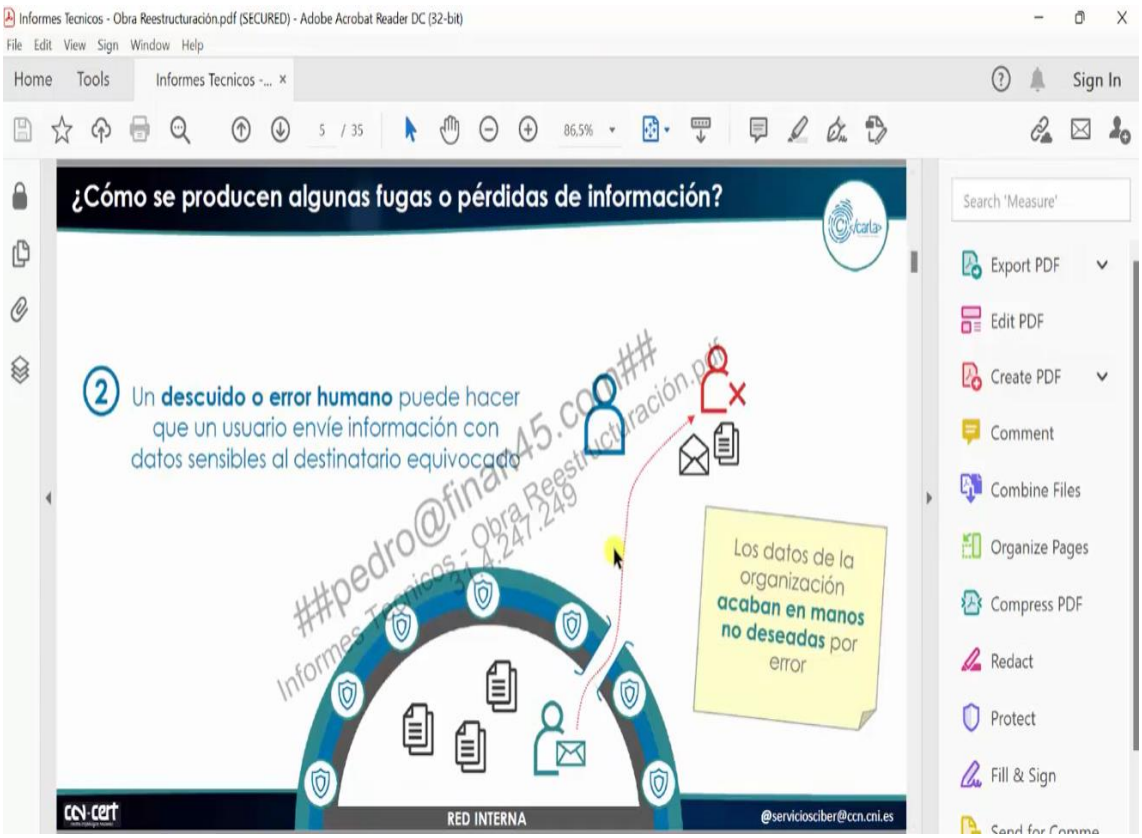
En Word:



24 Abriendo un fichero Word protegido CARLA con permisos.

Pero, en el caso de ficheros PDF se ha de tener en cuenta que sólo se ejecutarán correctamente en Suites de Pdf que soportan el estándar de seguridad por certificados, por ejemplo: Adobe reader, nitro, Nuance.

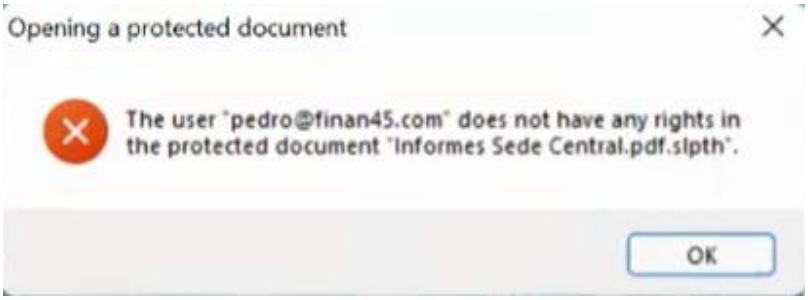
Los navegadores Chrome o Edge no soportan ese estándar y se debe cambiar a través del menú contextual a abrir con Acrobat.



25 Abriendo un fichero PDF protegido con CARLA.

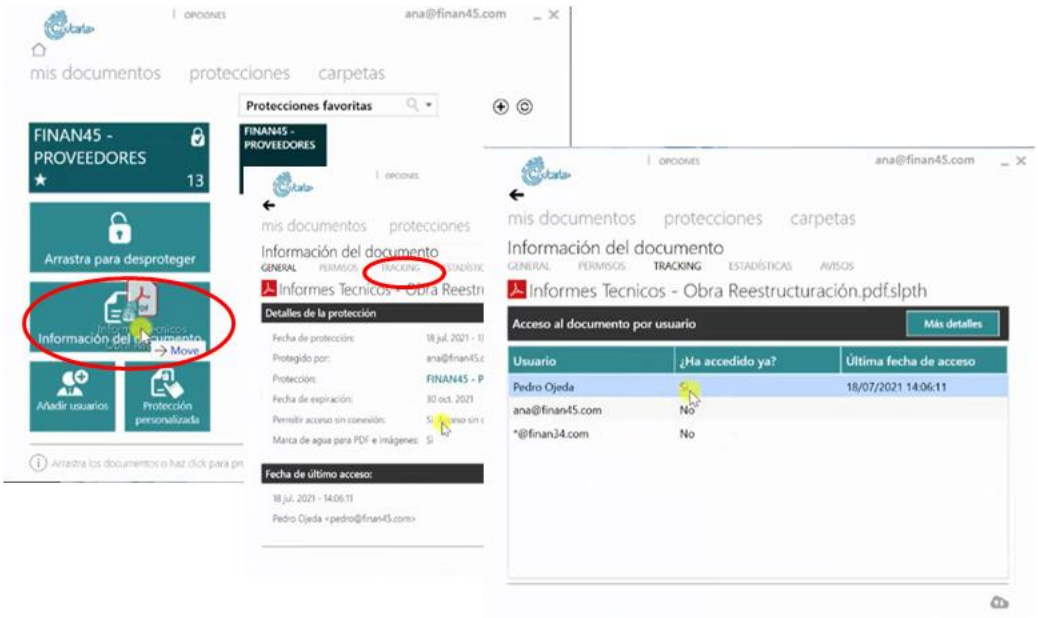
En este caso es un fichero pdf con marca de agua del correo del usuario, para que quede constancia de quién accede. Es una de las opciones que se pueden configurar en la política.

En el caso de intentar abrir un fichero sin permiso, quedará en *trazabilidad* y aparecerá el siguiente mensaje.



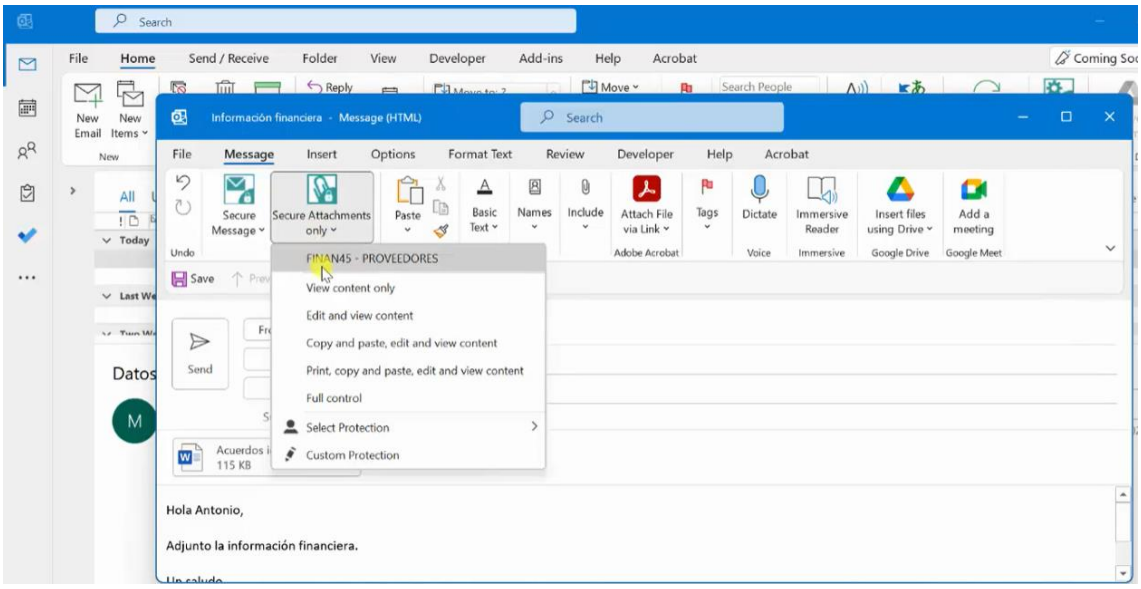
26Intento de acceso a fichero protegido con CARLA sin autorización.

Para ver la información del fichero, qué usuario lo protegió, sus accesos, bloquear el fichero para que no pueda ser accedido, etc., se deberá arrastrar el fichero a Información del documento.

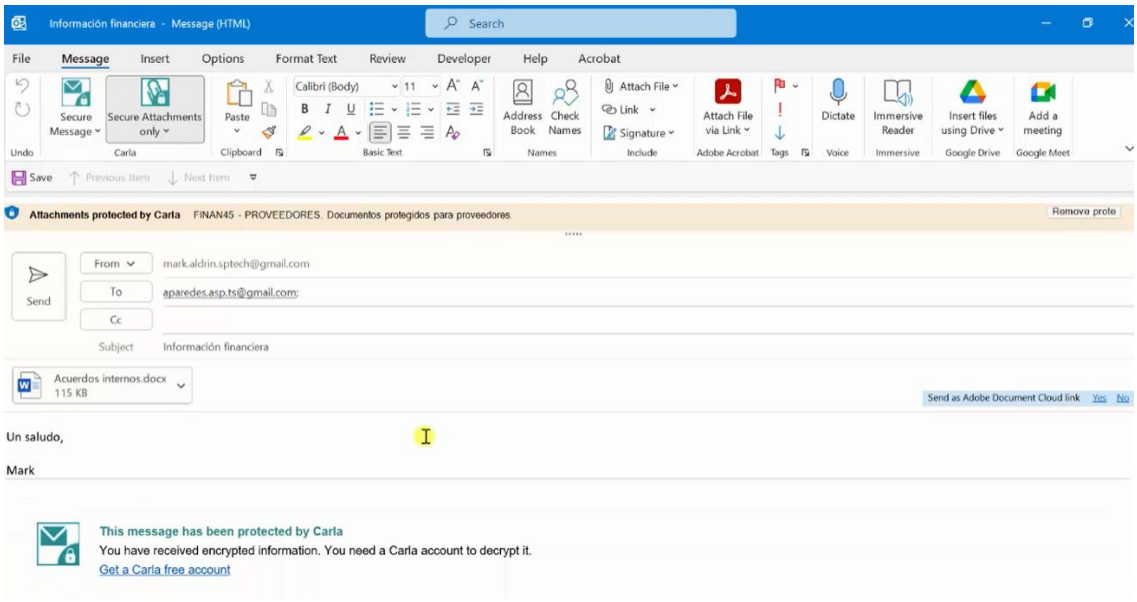


27 Información de protección del fichero y actividad.

Igual se pueden proteger los mensajes y sus anexos cuando viajan y salen de nuestra organización a usuarios externos. Si en la política se introduce un usuario que no pertenece a nuestra organización, se envía un mensaje para que se registre en CARLA, y de esa forma pueda acceder al fichero. Siempre se podrá bloquear e indicar su período de expiración.

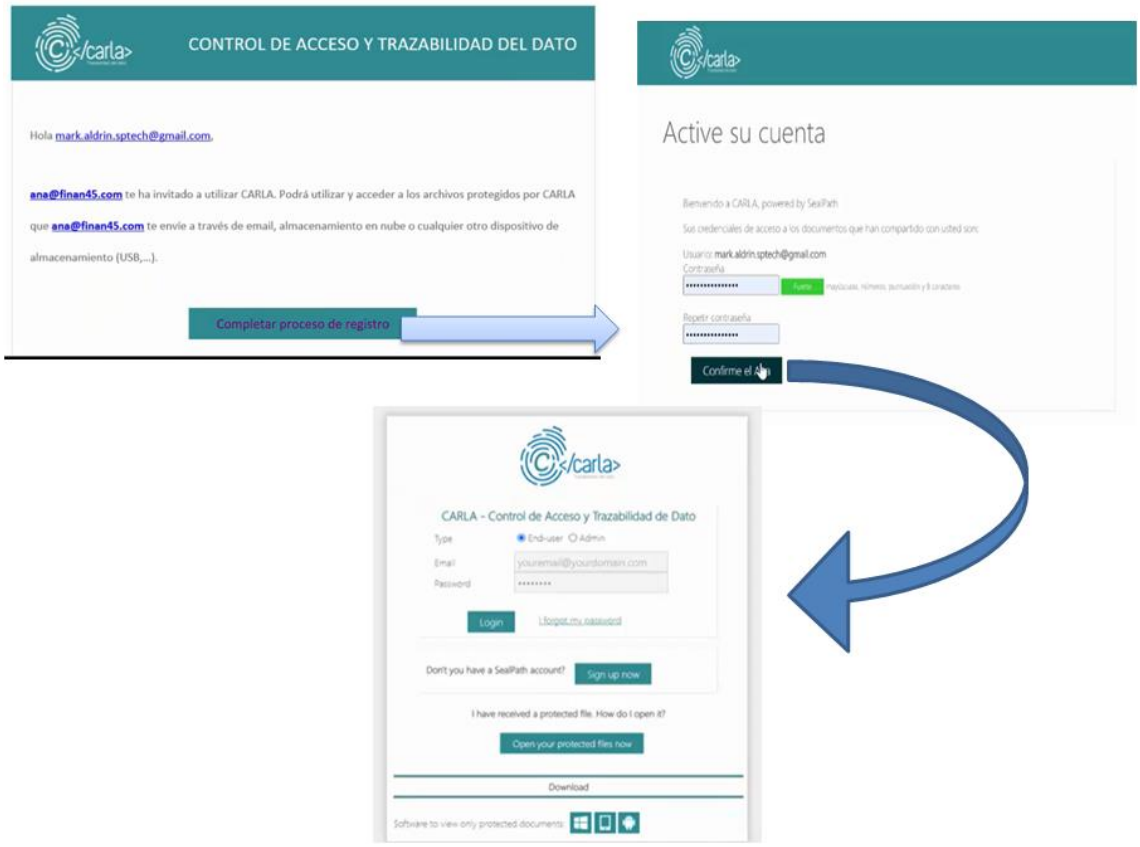


28 Protegiendo ficheros anexos a mensajes con Outlook mediante pluging.



29 Anexo protegido.

Este sería el aviso que le llegaría a un usuario externo para que se registre en CARLA y pueda validarse a través de CARLA LIVE.



30 Registro de usuario externo en CARLA y validación.

12. Herramienta para el ejercicio de los derechos.

Una de las cosas fundamentales que se obliga a los responsables del tratamiento es a la gestión de las solicitudes de los ciudadanos, con unos requisitos básicos como:

1) Plazo de contestación de un mes, prorrogable a dos meses previo informe al interesado de dicha prórroga.
2) Se debe informar sobre la no atención de la solicitud de ejercicio de derecho.
3) Toda solicitud es siempre gratuita.
4) Cuando se produzca una reiteración de solicitudes que sean infundadas o excesivas, podrá no actuarse respecto a la solicitud.
5) Se deben identificar los interesados o representantes.
6) El responsable del tratamiento de dato de carácter personal deberá responder a la solicitud de derechos y disponer de una prueba de haberlo hecho.
7) Se deberá generar un procedimiento de desarrollo, aprobados por la Oficina Central de LOPD y por el DPD, para definir por ejemplo:
   a) Número de tramitadores.
   b) Identificación de los responsables firmantes y tramitadores.
   c) Asignación del tramitador para cada solicitud.

La herramienta que se desarrolla en esta guía contiene todos los modelos necesarios, a juicio del autor, para responder a las solicitudes planteadas, que son:

1) Solicitud por canales no admitidos por el Organismo. En caso de que el ciudadano opte por presentarlo sin formato o canal indicado en el Organismo.
2) Solicitud para ejercicio del derecho de Acceso. Modelo para que el ciudadano pueda presentarlo.
3) Solicitud para ejercicio del derecho de Rectificación. Modelo para que el ciudadano pueda presentarlo.
4) Solicitud para ejercicio del derecho de Supresión. Modelo para que el ciudadano pueda presentarlo.
5) Solicitud para ejercicio del derecho Limitación del Tratamiento. Modelo para que el ciudadano pueda presentarlo.
6) Solicitud para ejercicio del derecho de Portabilidad de los datos. Modelo para que el ciudadano pueda presentarlo.
7) Solicitud para ejercicio del derecho de Oposición. Modelo para que el ciudadano pueda presentarlo.
8) Prórroga de dos meses en contestación.
9) Subsanación de falta de información.
10) Subsanación por falta de representación.
11) Subsanación por falta de firma.
12) Ejercicio del derecho de Acceso, no se tratan los datos.
13) Ejercicio del derecho de Acceso, donde sí se tratan los datos.
14) Ejercicio del derecho de Rectificación, no procede.
15) Ejercicio del derecho de Rectificación, procede.

16) Ejercicio del derecho de Supresión, no procede.
17) Ejercicio del derecho de Supresión, procede.
18) Ejercicio del derecho de Limitación del Tratamiento, no procede.
19) Ejercicio del derecho de Limitación del Tratamiento, procede.
20) Ejercicio del derecho de Portabilidad de los datos, no procede.
21) Ejercicio del derecho de Portabilidad de los datos, procede.
22) Ejercicio del derecho de Oposición, no procede.
23) Ejercicio del derecho de Oposición, procede.

La herramienta se ha desarrollado para que sea gratuita y no genere ningún tipo de coste adicional al Organismo. Se emplean las herramientas proporcionadas por el paquete Microsoft Office. Se acompaña a la memoria del TFG en formato comprimido RAR[2] y se ha de descomprimir en la raíz del disco C. Se creará una carpeta denominada **Herramienta PD**.

	MODELOS		
Ejercicio del derecho a:			
Solicitud por **canales no admitidos por el Organismo**. En caso de que el ciudadano opte por presentarlo sin formato o canal indicado en el Organismo.	Respuesta de redirección de la solicitud		
Solicitud para ejercicio del derecho de Acceso. Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No se tratan los datos	Sí se tratan los datos
Solicitud para ejercicio del derecho de **Rectificación.** Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No procede	Procede
Solicitud para ejercicio del derecho de Supresión. Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No procede	Procede
Solicitud para ejercicio del derecho **Limitación del Tratamiento**. Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No procede	Procede
Solicitud para ejercicio del derecho de **portabilidad de los datos**. Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No procede	Procede
Solicitud para ejercicio del derecho de **Oposición.** Modelo para que el ciudadano pueda presentarlo.	Modelo de solicitud	No procede	Procede
Prórroga de dos meses en contestación.	Modelo de prórroga		
Subsanación de falta de información.	Modelo subsanación falta información		
Subsanación por falta de representación.	Modelo subsanación falta de representación		
Subsanación de falta de firma.	Modelo de subsanación de falta firma		

33 Herramienta para responsable o encargado de tratamiento.

[2] Herramientas PD (google drive)

Conclusiones

Cuando se inició el presente TFG se marcaron unos objetivos primarios y otros secundarios. Los objetivos principales era desarrollar una guía sencilla, para que las figuras responsabilidad en el tratamiento de los DP pudieran cumplir, con facilidad, la observancia de los D y L fundamentales de los ciudadanos respectando la normativa actual, sabiendo realizar un análisis de riesgo apropiado para la protección de los datos personales y, por último, seleccionar medidas de seguridad, *salvaguardas* o controles que nos permitieran garantizar dichos D y L. En este último caso se ha presentado la solución más reciente para garantizar la privacidad de los DP y la trazabilidad, con CARLA. Se ha realizado un análisis de riesgo con la herramienta µPilar y se ha anexado al proyecto como Anexo I.

Hay que reconocer que ha llevado mucho tiempo familiarizarse con los nuevos conceptos de Seguridad y de análisis de riesgo. Se han llevado a cabo dos cursos de formación en CCN y, además, existía una gran documentación al respecto, guías, mejores prácticas, informes, etc., que han consumido gran parte del tiempo disponible de este TFG. No obstante, se han conseguido realizar los dos objetivos secundarios que en este proyecto se barajaban. El primero era una herramienta sencilla para comunicación con la persona física dentro de los tratamientos, que es algo que es obligatorio en todo organismo que trate con la protección de datos. El segundo, modelar una base de datos para un registro de actividades de tratamiento, que es obligatorio disponer también. Dicho esquema y su código SQL para poder crear la BBDD y sus tablas en un servidor SQL Server, se encuentran en el anexo II.

Hubiera sido muy interesante finalizar el RAT con servidor WEB en PHP, pero no ha sido posible en este TFG y pudiera ser una opción para un próximo Trabajo.

Glosario

Amenaza: Es la acción que puede llegar a ocurrir mediante la explotación de una vulnerabilidad.

Anonimización: Proceso por el que un conjunto de datos genera un nuevo conjunto, del cual no se puede obtener el original. No es posible la reidentificación.

Autenticidad: Dimensión de seguridad de un activo que permite identificar a la persona que lo está utilizando.

Cifrado homomórfico: técnica que permite realizar operaciones sobre los datos cifrados y obtener resultados, también cifrados, equivalentes a las operaciones realizadas directamente sobre la información original.

Confidencialidad: Dimensión de seguridad de un activo que consiste en ser usado solamente por aquellas entidades o personas autorizadas. Además, es una característica de seguridad consistente en que la información no se pone a disposición de procesos o individuos no autorizados.

Disponibilidad: La dimensión de seguridad de un activo que consiste en estar accesible para las personas que requieran su uso el mayor tiempo posible. Además, es una característica del activo consistente en que los procesos o individuos autorizados puedan acceder a él.

Incidente: Es la materialización de una amenaza que atenta contra cualquier dimensión de seguridad de un sistema.

Integridad: Dimensión y característica de seguridad de un activo que consiste en el mantenimiento del contenido de la información libre de modificaciones no autorizadas.

K-anonimidad: Propiedad de datos anonimizados que cuantifica la anonimidad de la persona cuando se han eliminado identificadores a un conjunto de datos.

Modelo de conocimiento cero.- Permiten la minimización en contexto distribuido y la limitación de accesibilidad a los datos.

Perjuicio: Daño causado a una organización o empresa al infringir la normativa.

Privacidad: Dimensión y característica de seguridad de un activo consistente en la capacidad de que sólo las personas o procesos autorizados puedan acceder a datos.

Resiliencia: Capacidad de un sistema para recuperarse tras un incidente. Dimensión en EIPD.

Salvaguarda: Medidas utilizadas para mitigar el impacto de posibles *amenazas* contempladas en el ENS.

Seudonimización: tratamiento de datos personales de manera que no puedan atribuirse a una persona física sin utilizar alguna información adicional, si ésta figura por separado y esté sujeta a medidas técnicas y organizativas para que no se atribuyan a una persona física identificada.

Sumarizar: No utilizar valores concretos en atributos. En su lugar usar rangos o intervalos.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, automatizados o no.

Trazabilidad: Dimensión y característica de seguridad de un activo que consiste en la capacidad de garantizar el "no repudio", esto es, poder identificar a la persona que haya utilizado el activo para cualquier fin.

Valor: Dimensión de seguridad de un activo consistente en el valor que posee para la empresa. A mayor valor, mayores las consecuencias de la pérdida del activo.

Vulnerabilidad: Fallo o error de configuración o error de programación del sistema, que, explotado convenientemente, puede convertirse en *amenaza*.

Acrónimos

AAPP.- Administraciones Públicas.

AD.- Directorio Activo.

AEPD.- Agencia Española de Protección de Datos, agencia de control en España para cumplir con el RGPD.

ARCO.- Derechos de Acceso, Rectificación, Cancelación y Oposición.

ARCO+.- Derechos ARCO más derechos de portabilidad, olvido o supresión y limitación.

ASS.- Administrador de Seguridad del Sistema, nivel operativo del ENS.

BBDD.- Base de Datos.

BOE.- Boletín Oficial del Estado.

CCN.- Centro Criptológico Nacional, encuadrado en el Centro Nacional de Inteligencia que, a su vez, se encuentra adscrito al Ministerio de Defensa.

CCN-CERT.- Equipos de respuesta a emergencias informáticas del Centro Criptológico Nacional.

D y L.- Derechos y Libertades.

DP.- Protección de datos.

DPD.- Delegado de protección de Datos, dentro del nivel de supervisión del ENS.

ENS.- Esquema Nacional de Seguridad, regulado en *Real Decreto 311/2022, de 3 de mayo*.

FR.- Factor de Riesgo.

INES.- Informa Nacional del Estado de Seguridad.

LDAP.- Protocolo de Acceso a Directorio Ligero.

LOPDGDD.-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LUCIA.- Listado Unificado de Coordinación de Incidentes y *Amenazas*.

MAGERIT.- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

NR.- Nivel de Riesgo.

NRT.- Nivel de Riesgo del Tratamiento.

POS.- Procedimientos operativos de seguridad.

RAT.- Registro de Actividad de Tratamientos.

RD.- Real Decreto.

RGPD.-Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo en relación a la protección y libre circulación de datos.

RSEG.- Responsable de Seguridad según el ENS, nivel supervisión del ENS.

RSIS.- Responsable del Sistema, nivel operativo del ENS.

SARA.- Sistemas de Aplicaciones y Redes para las Administraciones.

SAT-INET.- Sistema de Alerta Temprana de Internet.

SAT-SARA.- Sistema de Alerta Temprana de Red SARA.

TFG.- Trabajo Fin de Grado.

TIC.- Tecnologías de la Información y la Comunicación.

UE.- Unión Europea.

Bibliografía y referencias.

1. *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común.* s.l. : BOE, 2015.

2. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. s.l. : BOE, 2015.

3. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. s.l. : BOE, 2022.

4. Reglamento 2016/679 del Parlamento Europeo y del Consejo en relación a la protección y libre circulación de datos. s.l. : UE, 2016.

5. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. s.l. : BOE, 2018.

6. **CCN.** Adecuación al ENS para Universidades. 2022. Vol. Guía de Seguridad, CCN-STIC 881.

7. **Datos, Agencia Española de Protección de.** Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. s.l. : AEPD, 2021.

8. **CCN.** *Informe anual Marco Normativo y salvaguardas.* 2020. 14.

9. **Datos, Agencia Española de Protección de.** *Memoria Anual de actividad.* s.l. : AEPD, 2021.

10. —. *Guía privacidad desde el diseño.* s.l. : AEPD, 2019.

Anexo I. Análisis de riesgo con µPilar.

Introducción

Como ya se ha expuesto en el capítulo Análisis de riesgo, es fundamental realizar una evaluación sobre el riesgo que puede afectar el sistema de información así como realizar una evaluación del impacto en protección de datos personales.

µpilar, es una versión de Pilar, que es una herramienta creada por el CCN que permite a una organización realizar una evaluación de riesgos que pueden suceder en su sistema de información homogéneo en el planteamiento de su seguridad y sugerir una serie de medidas con el objetivo de poder reducir la probabilidad de que esos riesgos se materialicen. Se puede descargar gratuitamente desde la página PILAR - Inicio (cni.es)(https://pilar.ccn-cert.cni.es/). Funciona con una licencia que se puede obtener, gratuita para las AAPP, contactando con el siguiente correo pilar@ccn-cert.cni.es.

En esta guía se va a describir un proyecto ejemplo con el objetivo de explicar sus pasos y cómo interpretar los datos del análisis. También se detallará como construir informes usando la aplicación sobre los riesgos de la organización.

Proyecto ejemplo

Lo primero que se encuentra al crear un nuevo proyecto es la pantalla de datos, en la que se pide una serie de datos que figurarán en el informe.

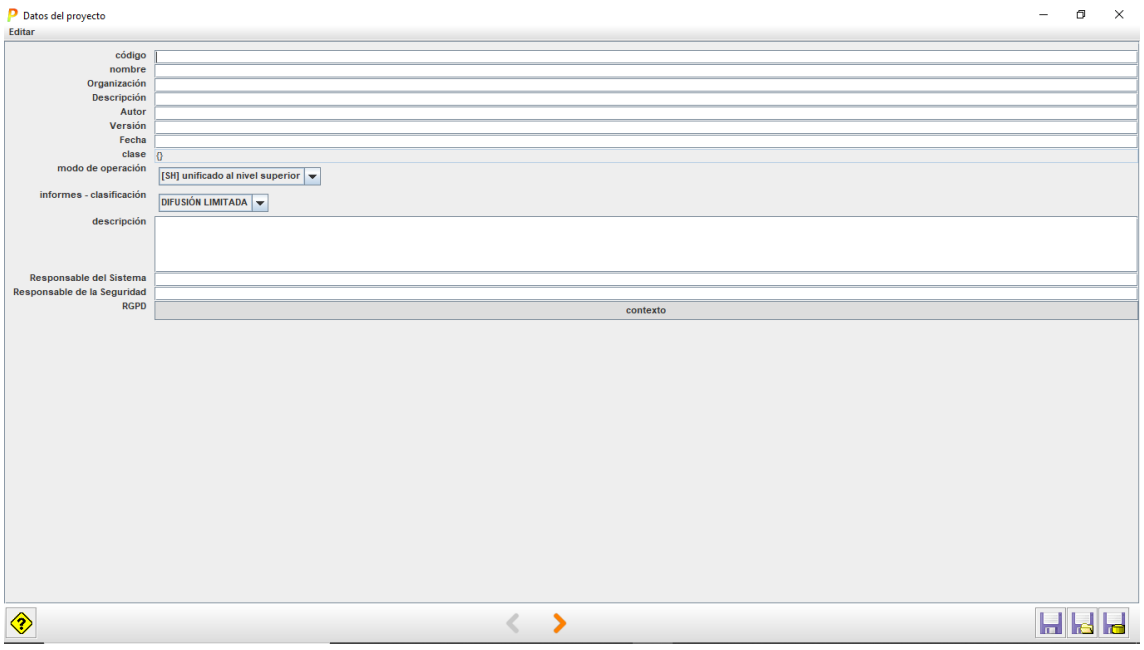


Figura 1: Datos del proyecto en µPilar

Los campos son bastante intuitivos, y se rellenan fácilmente. No obstante, es necesario especificar los siguientes:

- Clase: El grado de cumplimiento en lo referente al marco del ENS y el contexto de seguridad de la organización.
- Modo de operación: El modo que utilizan los sistemas seguros para el tratamiento de datos o información clasificada.
- Informes-clasificación: La clasificación respecto al nivel de *confidencialidad* del informe.
- RGPD: Aquí se definirá todo el contexto sobre el RGPD, desde los roles del tratamiento, hasta la necesidad de la EIPD o la justificación normativa y proporcionalidad del tratamiento, pasando por su ciclo de vida.

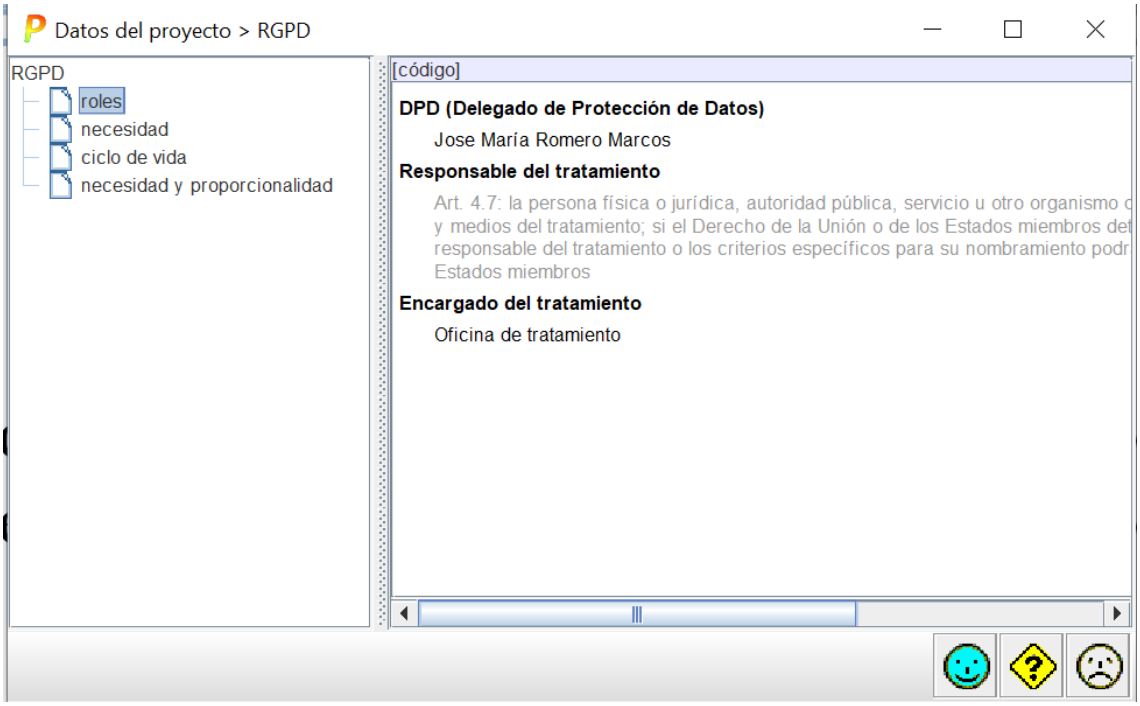


Figura 2: Definición del contexto RGPD en µPilar

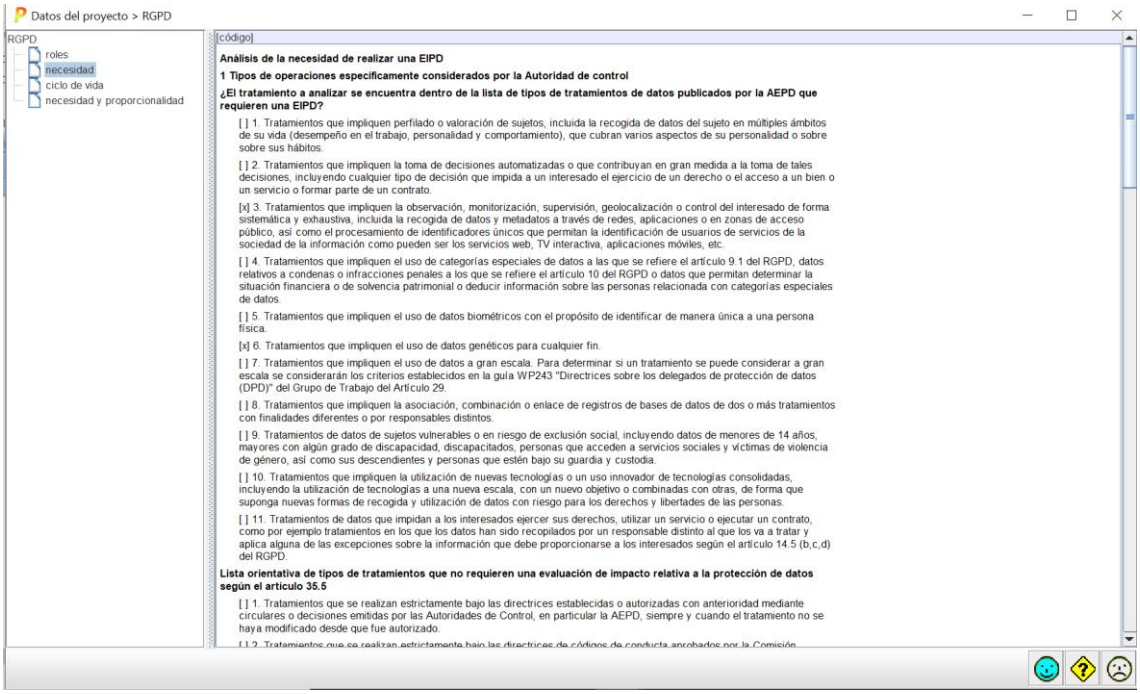


Figura 3: Análisis de la necesidad de EIPD

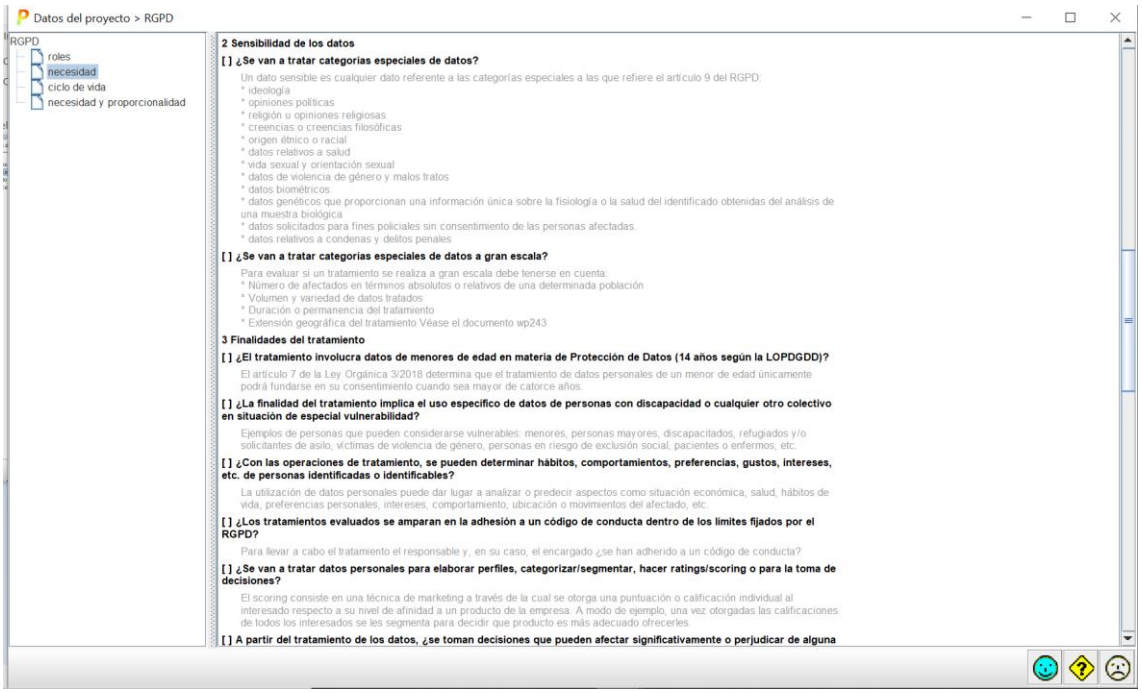


Figura 4: Tipo de datos y finalidad del tratamiento de datos de carácter personal.

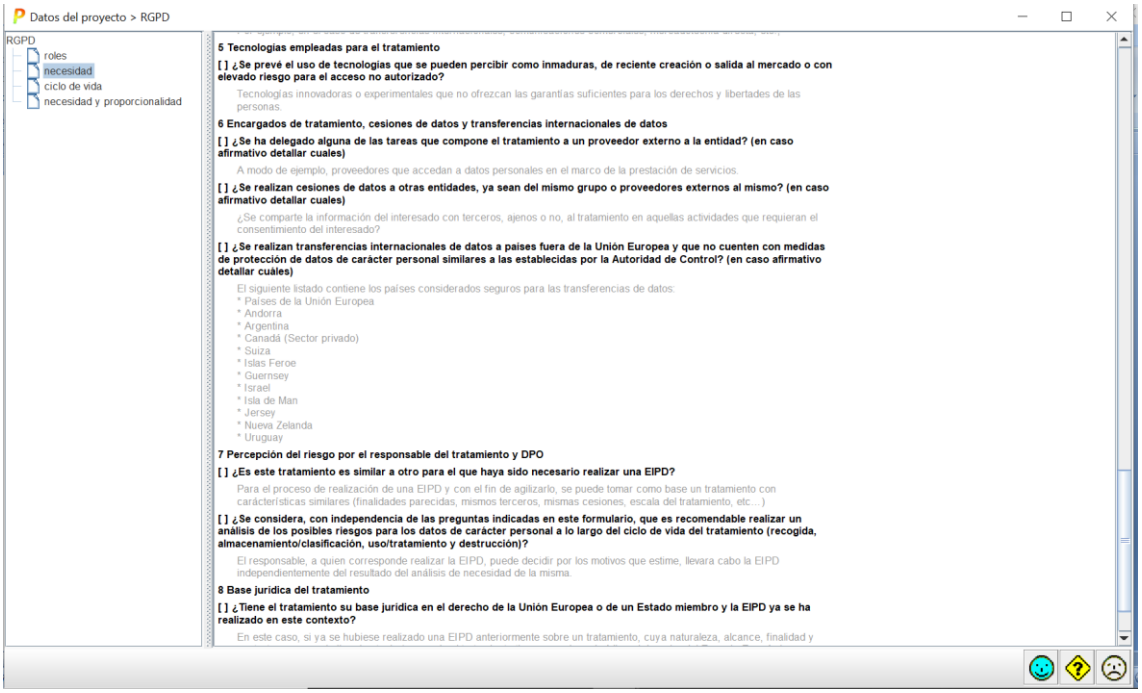


Figura 5: Tecnologías, percepción del riesgo y Base Jurídica RGPD

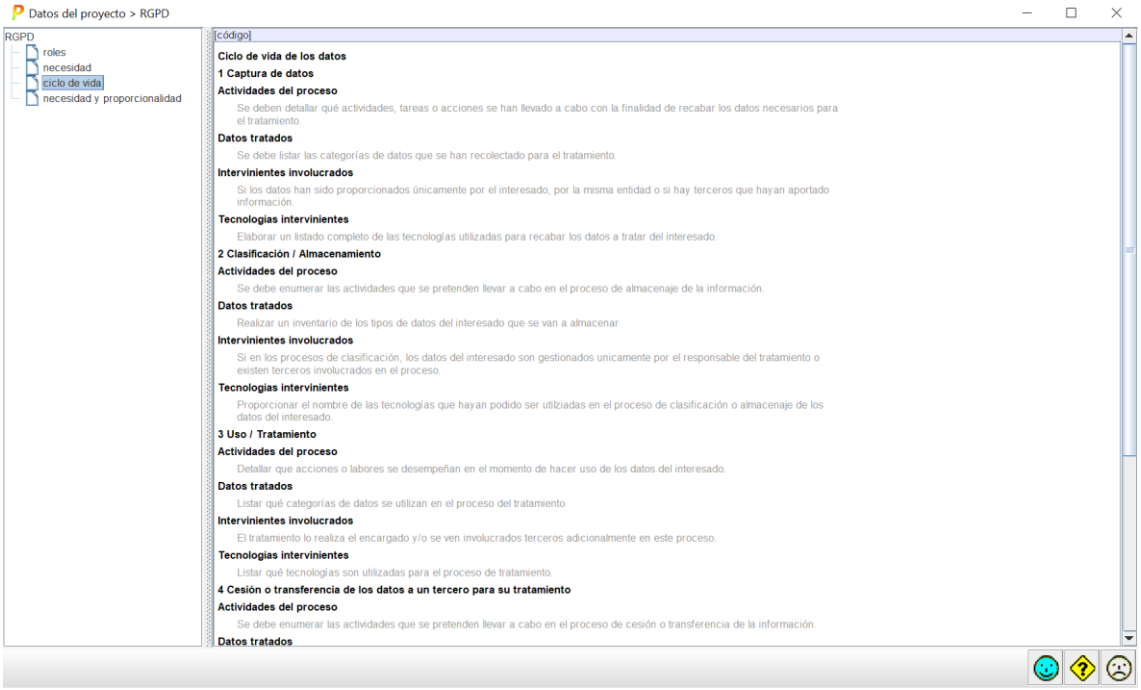


Figura 6: Ciclo de vida del tratamiento de datos

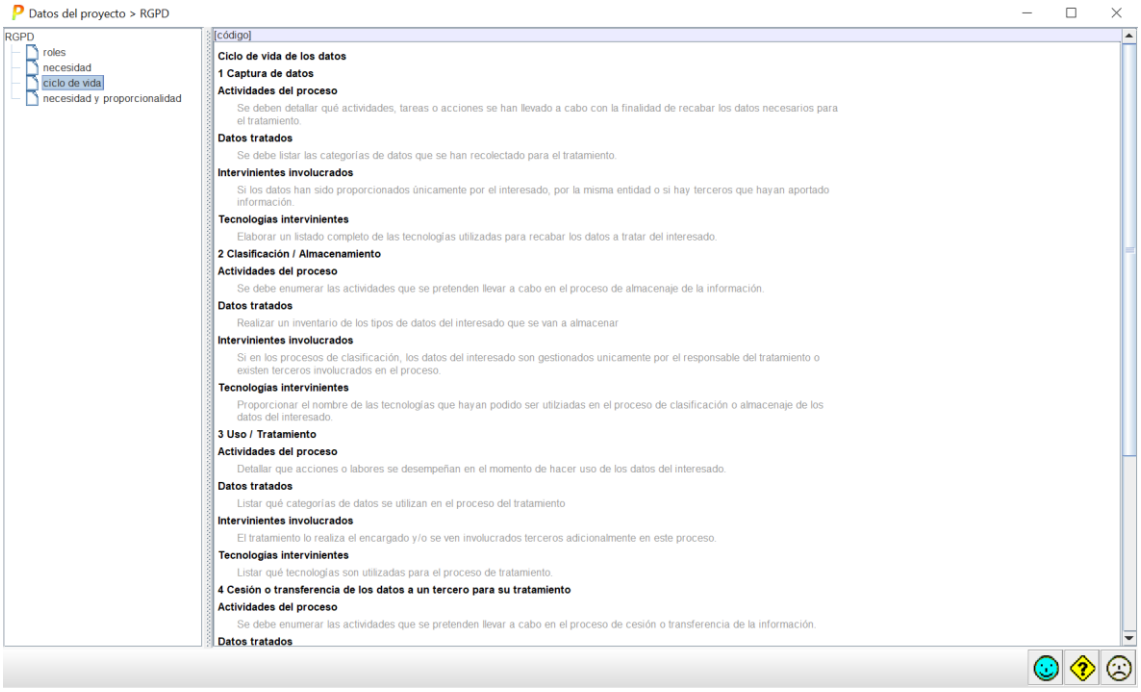


Figura 7: Análisis de la necesidad y proporcionalidad del tratamiento.

Es destacable mencionar que se pueden cambiar las descripciones de estos campos. Esto es útil para poder definir, por ejemplo, en la sección de roles a las entidades o individuos que se encarguen de los tratamientos.

Una vez creado el proyecto, se solicitará que se especifiquen los diferentes activos que tengamos en la empresa y el impacto de las dimensiones en cada uno.

Se pueden diferenciar cuatro tipos de activos:

- Activos esenciales: Estos son los activos fundamentales del sistema. En este campo se definen los servicios que da la organización y la información que tiene. Por ejemplo, los expedientes de usuarios o los servicios de tramitación que se pueden dar.
- Sistemas de protección de frontera lógica: Son los elementos del sistema que protegen los activos desde el punto de vista lógico. Un antivirus o un cortafuegos podrían pertenecer a esta categoría.
- Sistemas de protección de frontera físico: Son los elementos del sistema que protegen los activos desde el punto de vista físico. Las oficinas y los espacios de trabajo donde se guarda la información podrían pertenecer a esta categoría.
- Contratados a terceros: Son aquellos elementos que se requieren para el tratamiento y gestión de los activos y que se contratan a otra compañía, como, por ejemplo, la conexión a Internet.

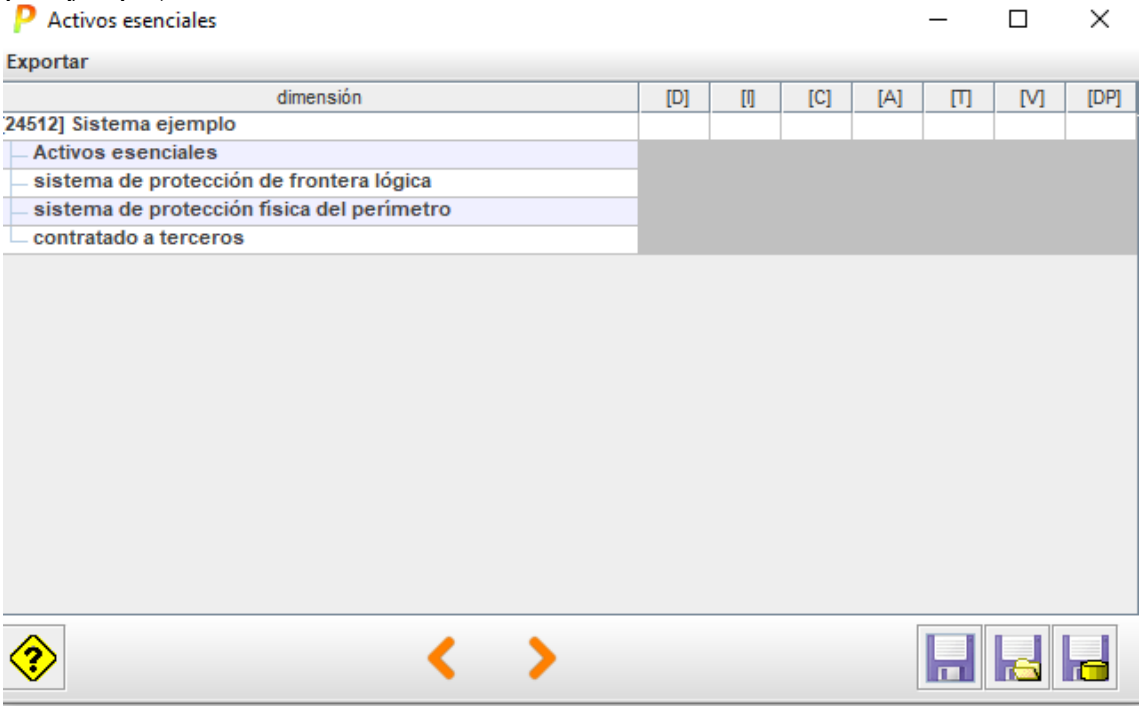


Figura 8: Ventana de activos y dimensiones

Para añadir todos estos activos, se debe hacer clic derecho sobre la categoría que se vaya a añadir y elegir “nuevo activo”. Aparecerá una ventana donde se podrán introducir los datos del activo. Tras hacer clic al botón “OK”, el código y nombre del activo aparecerán en la categoría deseada.

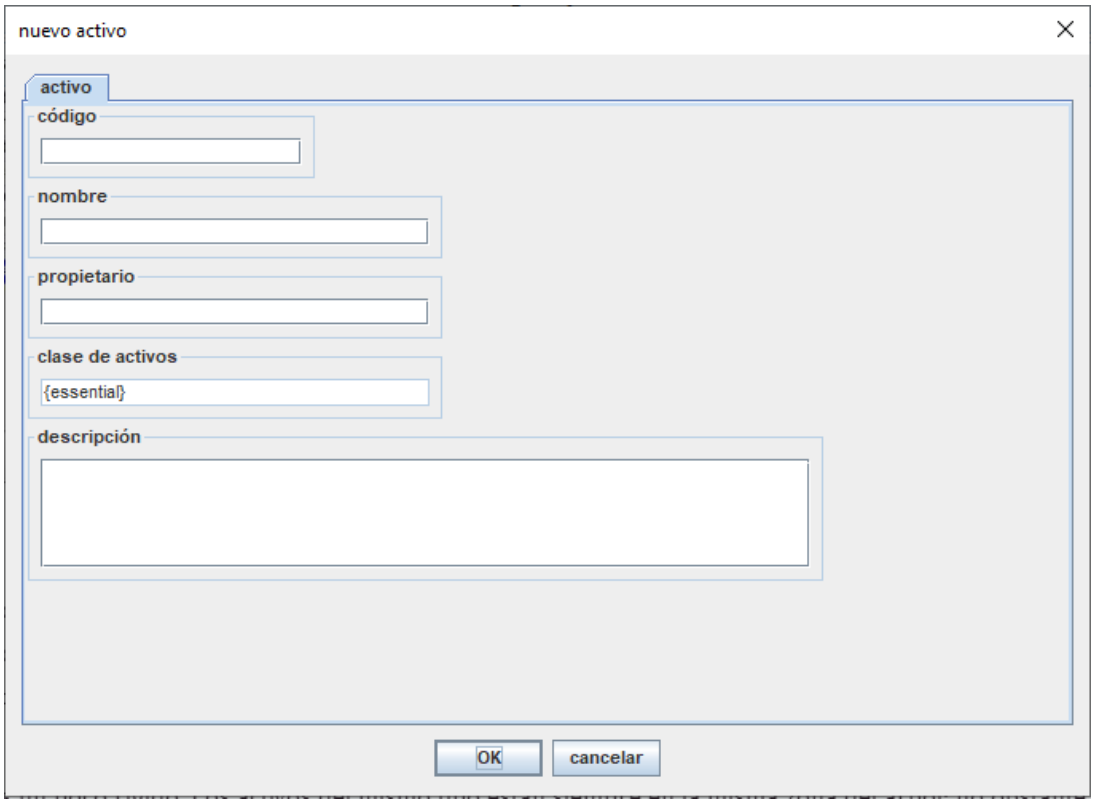


Figura 9: Creación de nuevos activos en PILAR

Una vez definidos los activos, se debe valorar el nivel requerido de seguridad para cada una de las columnas que tienen al lado. Cada columna corresponde a una dimensión del activo.

- D: *Disponibilidad*
- I: *Integridad*
- C: *Confidencialidad*
- A: *Autenticidad*
- T: *Trazabilidad*
- V: *Valor*
- DP: *Privacidad*

Si se hace clic en la casilla de una dimensión del activo a valorar, aparecerá la siguiente ventana:

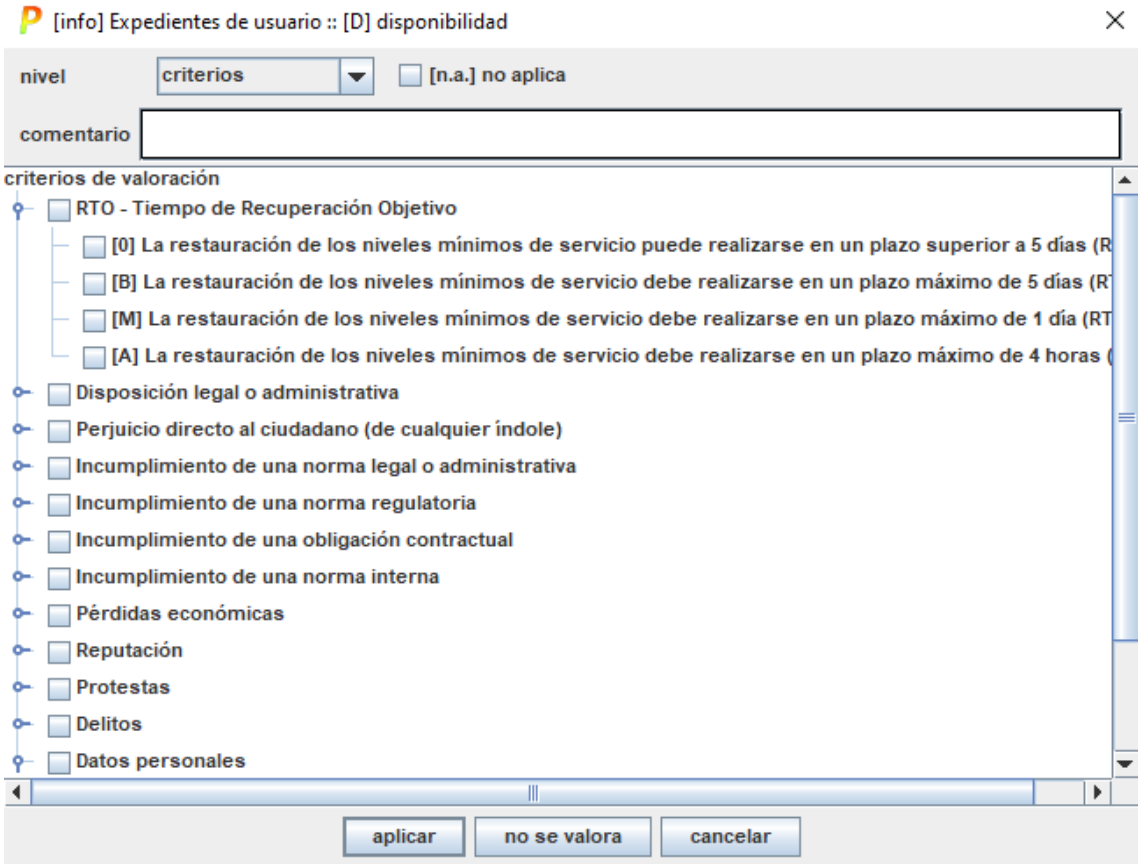
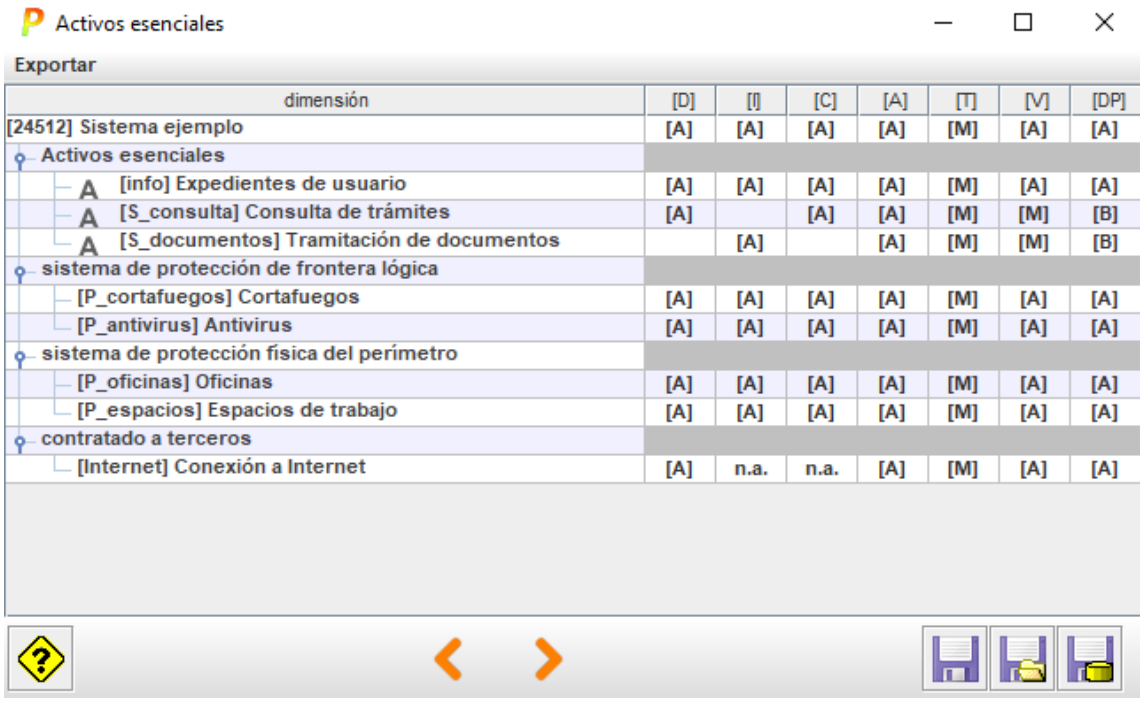


Figura 10: Valoración de dimensiones

En dicha ventana se deben escoger aquellos criterios o consecuencia que pueden surgir al no poner medidas para proteger esta dimensión. Por ejemplo, el tiempo de recuperación en caso de catástrofe o si un ataque exitoso podría generar un prejuicio o, simplemente, el dejar desprotegida dicha dimensión conllevaría al incumplimiento de una norma y, por tanto, a una compensación económica o pérdida de alguna licencia para el tratamiento de los datos. Todos los criterios tienen cuatro valores que por orden de peso son: [0] → [B] → [M] →[A]. También es posible indicar que la dimensión para este activo no es aplicable, ya que no se ve afectado por este. En ese caso, se puede usar el botón "no se valora".

Una vez se han escogido los criterios y se le ha dado a "aplicar", se verá que en la columna sale uno de los niveles explicados anteriormente. Siempre se escogerá el mayor nivel de todos los que hay para seleccionar el nivel de valoración general de dicha dimensión, es decir, si existen varios criterios con una valoración [B] y otros con una valoración [A] en la dimensión de DP, la valoración final será [A].



dimensión	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[24512] Sistema ejemplo	[A]	[A]	[A]	[A]	[M]	[A]	[A]
Activos esenciales							
[info] Expedientes de usuario	[A]	[A]	[A]	[A]	[M]	[A]	[A]
[S_consulta] Consulta de trámites	[A]		[A]	[A]	[M]	[M]	[B]
[S_documentos] Tramitación de documentos		[A]		[A]	[M]	[M]	[B]
sistema de protección de frontera lógica							
[P_cortafuegos] Cortafuegos	[A]	[A]	[A]	[A]	[M]	[A]	[A]
[P_antivirus] Antivirus	[A]	[A]	[A]	[A]	[M]	[A]	[A]
sistema de protección física del perímetro							
[P_oficinas] Oficinas	[A]	[A]	[A]	[A]	[M]	[A]	[A]
[P_espacios] Espacios de trabajo	[A]	[A]	[A]	[A]	[M]	[A]	[A]
contratado a terceros							
[Internet] Conexión a Internet	[A]	n.a.	n.a.	[A]	[M]	[A]	[A]

Figura 11: Ejemplo de valoración de dimensiones

Una vez se han valorado todas las dimensiones, el programa solicitará que se marquen otros activos que pudieran ser interesantes para el análisis y que apoyen las actividades de los activos esenciales que se han valorado anteriormente.

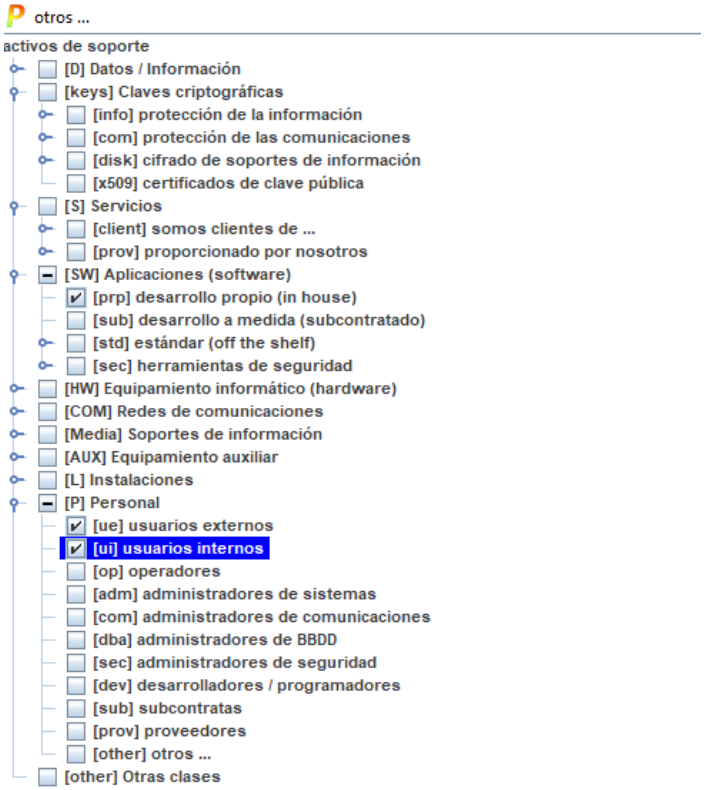


Figura 12: Ventana de activos de soporte

Una vez se han definido todos los activos presentes en el análisis, es necesario tener en cuenta aquellos factores agravantes que pueden poner en riesgo las funciones del proyecto. Entre estos factores hay que considerar una gran cantidad de riesgos: motivación de posibles atacantes, formación del personal, el grado de dependencia a Internet de los equipos, etc.

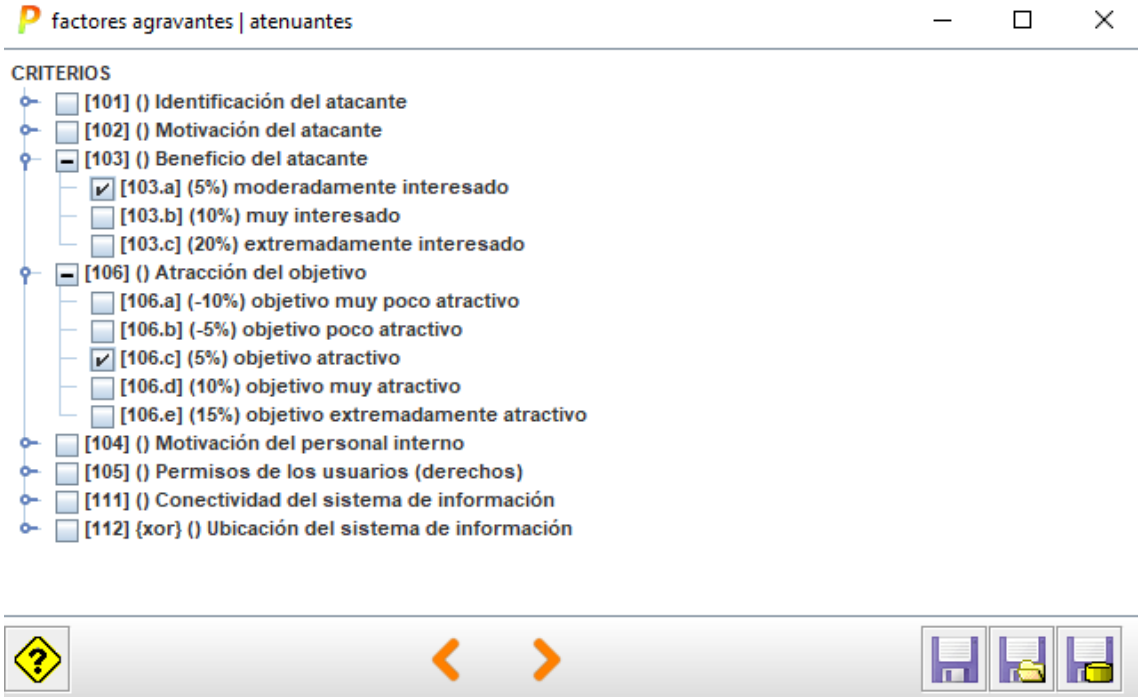


Figura 13: Factores agravantes

En este punto ya se conocen los activos de los que disponemos y que es necesario elegir el perfil de seguridad y las medidas para el tratamiento de riesgos que se van a emplear. Por defecto, la casilla de "Pilar: salvaguardas" ya viene marcada. Estas *salvaguardas* no son más que una serie de medidas que se verán más adelante para mitigar la materialización de las *amenazas* o el impacto que pudieran causar.

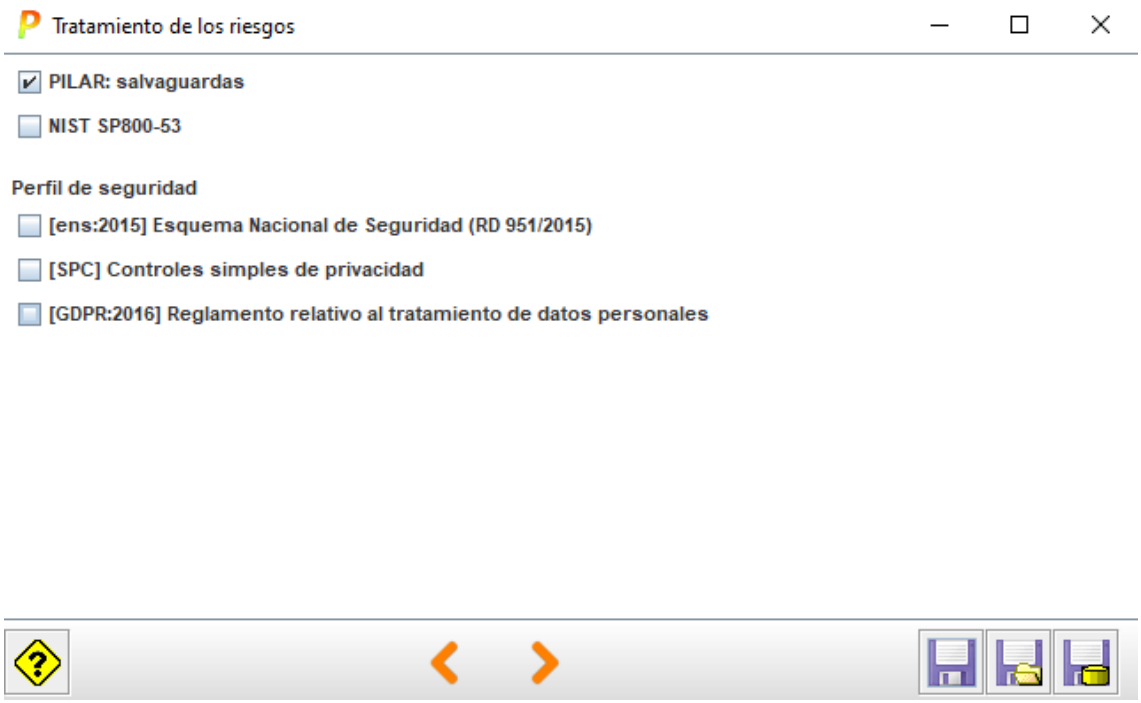


Figura 14: Perfil de seguridad y tratamiento de riesgos

Tras introducir todos estos datos, el programa extraerá una serie de riesgos clasificados del 1 al 10 y que reflejan el posible impacto de estos en las dimensiones de cada activo que hemos definido anteriormente. Es posible, además, observar el motivo por el cual existen tales riesgos, como, por ejemplo, que en el firewall sea posible la inyección de código malicioso.

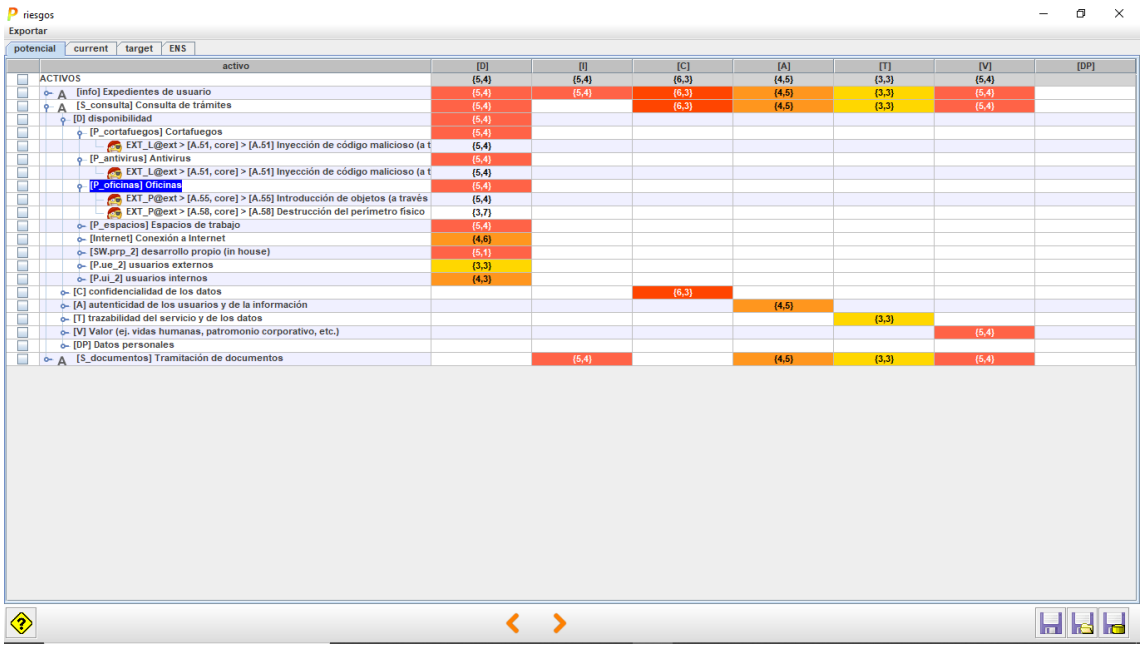
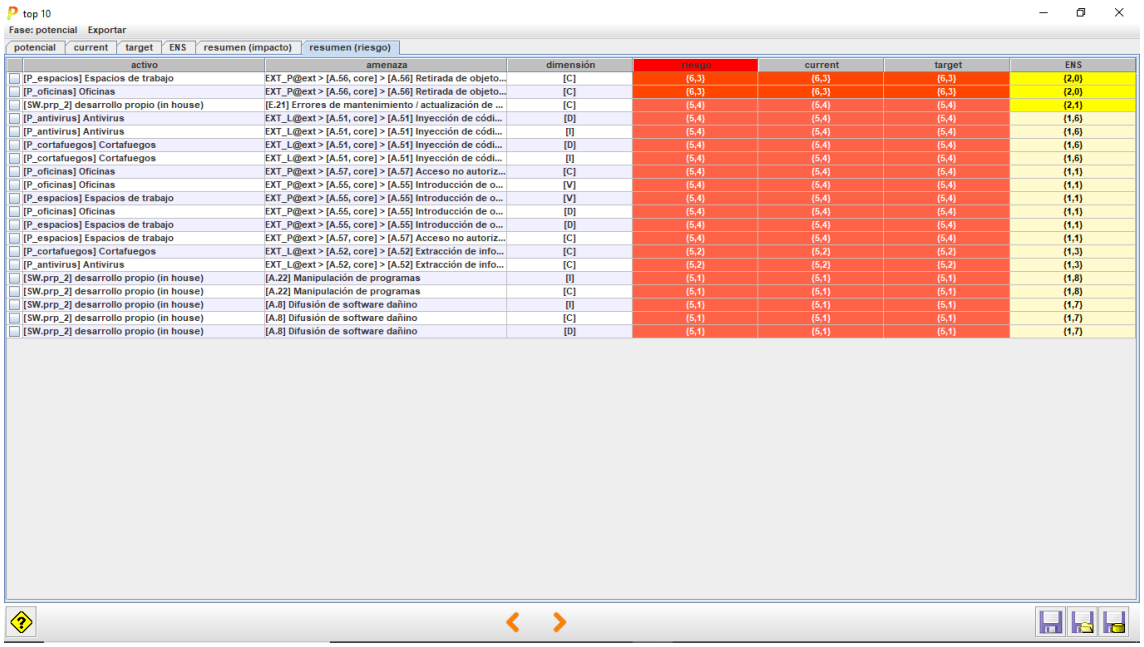


Figura 15: Riesgos potenciales de los activos introducidos

Con la intención de ayudar a centrarse en aquellos riesgos que pudieran causar más problemas, si se continúa a la siguiente ventana, Pilar mostrará los 10 riesgos con un mayor impacto en caso de materializarse. En esta ventana hay un total de seis pestañas, de las cuales son destacables especialmente los resúmenes de riesgo y de impacto.

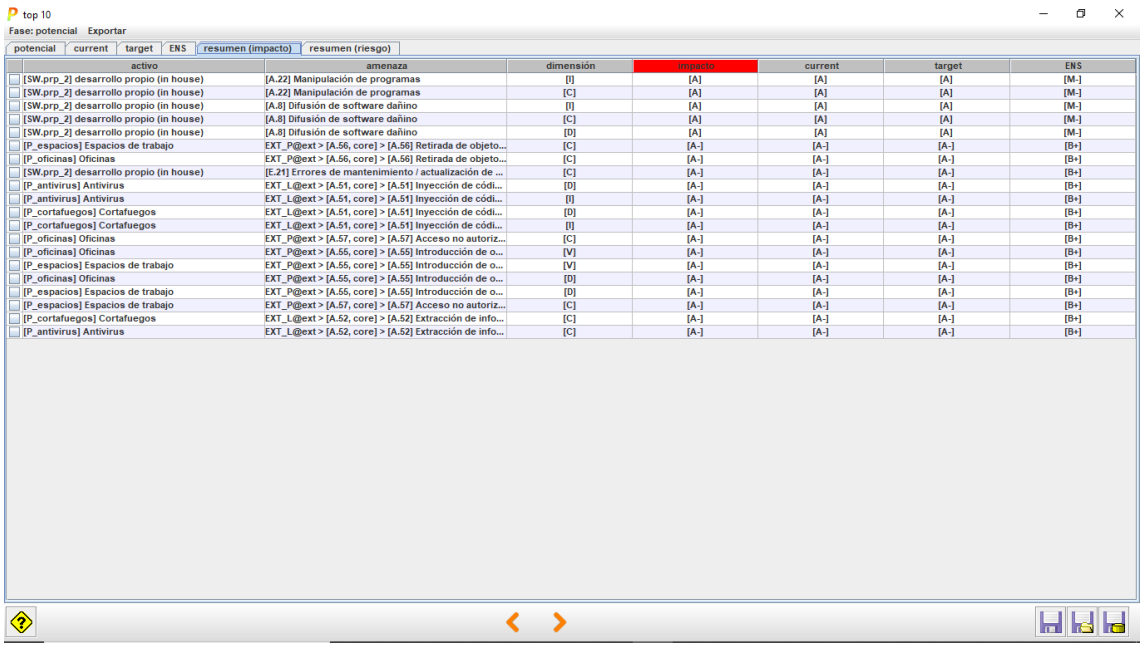
La que aparece por defecto es el resumen de riesgo, donde se ordenan los 10 riesgos más importantes que hay y la dimensión a la que afecta, mostrando en la última columna de la tabla como se puede mitigar el riesgo si se aplican las medidas establecidas por el ENS.



activo	amenaza	dimensión	riesgo	current	target	ENS
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.56, core] > [A.56] Retirada de objeto...	[C]	(6,3)	(6,3)	(6,3)	(2,0)
[P_oficinas] Oficinas	EXT_P@ext > [A.56, core] > [A.56] Retirada de objeto...	[C]	(6,3)	(6,3)	(6,3)	(2,0)
[SW.prp_2] desarrollo propio (in house)	[E.21] Errores de mantenimiento / actualización de ...	[C]	(5,4)	(5,4)	(5,4)	(2,1)
[P_antivirus] Antivirus	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[D]	(5,4)	(5,4)	(5,4)	(1,6)
[P_antivirus] Antivirus	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[I]	(5,4)	(5,4)	(5,4)	(1,6)
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[D]	(5,4)	(5,4)	(5,4)	(1,6)
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[I]	(5,4)	(5,4)	(5,4)	(1,6)
[P_oficinas] Oficinas	EXT_P@ext > [A.57, core] > [A.57] Acceso no autoriz...	[C]	(5,4)	(5,4)	(5,4)	(1,1)
[P_oficinas] Oficinas	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[V]	(5,4)	(5,4)	(5,4)	(1,1)
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[V]	(5,4)	(5,4)	(5,4)	(1,1)
[P_oficinas] Oficinas	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[D]	(5,4)	(5,4)	(5,4)	(1,1)
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[D]	(5,4)	(5,4)	(5,4)	(1,1)
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.57, core] > [A.57] Acceso no autoriz...	[C]	(5,4)	(5,4)	(5,4)	(1,1)
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.52, core] > [A.52] Extracción de info...	[C]	(5,2)	(5,2)	(5,2)	(1,3)
[P_antivirus] Antivirus	EXT_L@ext > [A.52, core] > [A.52] Extracción de info...	[C]	(5,2)	(5,2)	(5,2)	(1,3)
[SW.prp_2] desarrollo propio (in house)	[A.22] Manipulación de programas	[I]	(5,1)	(5,1)	(5,1)	(1,8)
[SW.prp_2] desarrollo propio (in house)	[A.22] Manipulación de programas	[C]	(5,1)	(5,1)	(5,1)	(1,8)
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[I]	(5,1)	(5,1)	(5,1)	(1,7)
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[C]	(5,1)	(5,1)	(5,1)	(1,7)
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[D]	(5,1)	(5,1)	(5,1)	(1,7)

Figura 16: Resumen de los 10 principales riesgos

La segunda pestaña, que adquiere mucha importancia en nuestro análisis, es la del resumen del impacto, donde se hace una valoración del nivel de riesgo a base de letras (A → alta, M →Media, B → Bajo) de la importancia del impacto de estos riesgos. De nuevo, se muestra la dimensión que afecta y como se podría mitigar aplicando lo establecido en el ENS.



activo	amenaza	dimensión	impacto	current	target	ENS
[SW.prp_2] desarrollo propio (in house)	[A.22] Manipulación de programas	[I]	[A]	[A]	[A]	[M-]
[SW.prp_2] desarrollo propio (in house)	[A.22] Manipulación de programas	[C]	[A]	[A]	[A]	[M-]
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[I]	[A]	[A]	[A]	[M-]
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[C]	[A]	[A]	[A]	[M-]
[SW.prp_2] desarrollo propio (in house)	[A.8] Difusión de software dañino	[D]	[A]	[A]	[A]	[M-]
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.56, core] > [A.56] Retirada de objeto...	[C]	[A-]	[A-]	[A-]	[B+]
[P_oficinas] Oficinas	EXT_P@ext > [A.56, core] > [A.56] Retirada de objeto...	[C]	[A-]	[A-]	[A-]	[B+]
[SW.prp_2] desarrollo propio (in house)	[E.21] Errores de mantenimiento / actualización de ...	[C]	[A-]	[A-]	[A-]	[B+]
[P_antivirus] Antivirus	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[D]	[A-]	[A-]	[A-]	[B+]
[P_antivirus] Antivirus	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[I]	[A-]	[A-]	[A-]	[B+]
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[D]	[A-]	[A-]	[A-]	[B+]
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.51, core] > [A.51] Inyección de códi...	[I]	[A-]	[A-]	[A-]	[B+]
[P_oficinas] Oficinas	EXT_P@ext > [A.57, core] > [A.57] Acceso no autoriz...	[C]	[A-]	[A-]	[A-]	[B+]
[P_oficinas] Oficinas	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[V]	[A-]	[A-]	[A-]	[B+]
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[V]	[A-]	[A-]	[A-]	[B+]
[P_oficinas] Oficinas	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[D]	[A-]	[A-]	[A-]	[B+]
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.55, core] > [A.55] Introducción de o...	[D]	[A-]	[A-]	[A-]	[B+]
[P_espacios] Espacios de trabajo	EXT_P@ext > [A.57, core] > [A.57] Acceso no autoriz...	[C]	[A-]	[A-]	[A-]	[B+]
[P_cortafuegos] Cortafuegos	EXT_L@ext > [A.52, core] > [A.52] Extracción de info...	[C]	[A-]	[A-]	[A-]	[B+]
[P_antivirus] Antivirus	EXT_L@ext > [A.52, core] > [A.52] Extracción de info...	[C]	[A-]	[A-]	[A-]	[B+]

Figura 17: Resumen de los 10 riesgos con mayor impacto

Cabe destacar que estas ventanas son puramente informativas sobre los riesgos al que nuestro sistema de información se enfrenta, y no será posible modificar ninguno de estos datos.

En la siguiente ventana, se ofrecerá la posibilidad de crear dos informes: El análisis de riesgo y el informe INES.

- El análisis de riesgo plasma todo lo que se ha anteriormente en las diferentes ventanas de la aplicación en un documento de texto bien formado que muestra los riesgos existentes y la explicación de los activos, todo dispuesto según los datos que se han introducido en la aplicación.

- El informe INES es un modelo para realizar informes de seguridad que el CCN ha creado y ha introducido en Pilar. Para poder leerlo en su totalidad, es necesario tener la herramienta INES, pero si se abre en un Excel, se puede ver que la intención es realizar un esquema con los riesgos más importantes, la valoración de impacto de cada dimensión, y las soluciones que desde el ENS se proponen.

Para terminar con el análisis de esta aplicación, µPilar sugiere una serie de medidas que se pueden utilizar para mitigar los riesgos presentados y mejorar la seguridad de la organización. Para ello presenta una lista de lo que se denominan *salvaguardas*. Cada uno de estos elementos tiene asociado una categoría especificada mediante su acrónimo, un nivel de recomendación del 1 al 10, un color de paraguas que muestra la importancia de cada *salvaguarda* para la organización y un nivel de madurez según la clasificación de medidas de seguridad del ENS (o un n.a si la medida, aunque pudiera ser interesante analizarla, no aplica para las necesidades de la organización o el proyecto). Investiguemos con mayor detalle esta ventana.

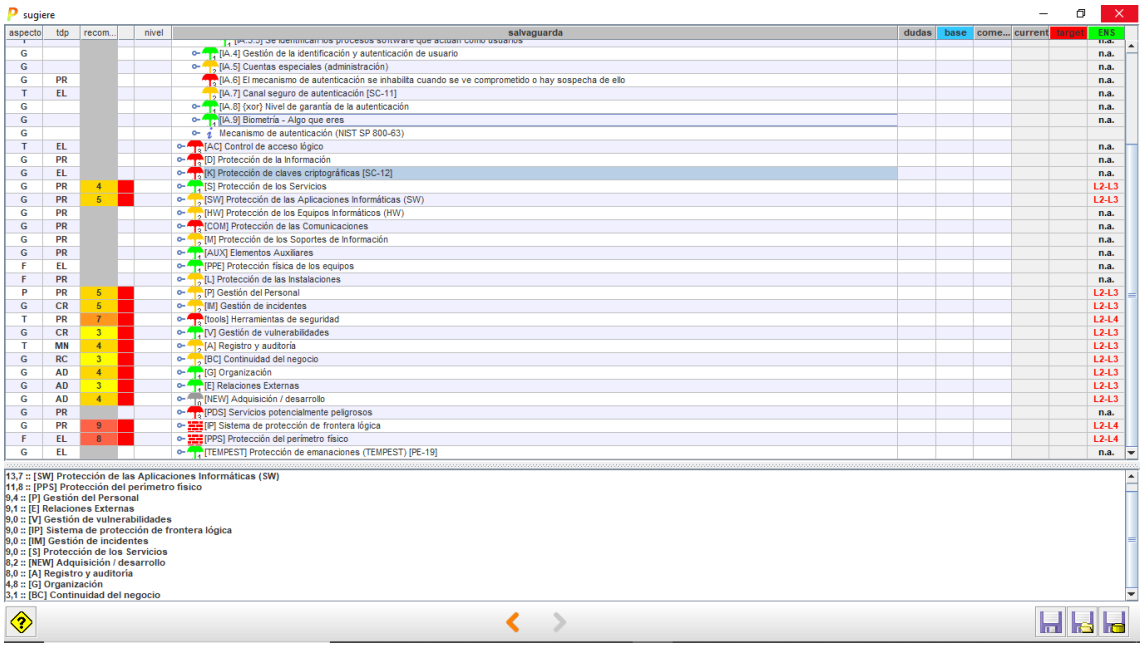


Figura 18: Sugerencia de salvaguardas de Pilar

La columna catalogada como tdp hace referencia a la categoría a la que pertenece cada una de las *salvaguardas*. Tenemos distintas clasificaciones:

- PR: Prevención
- DR: Disuasión
- EL: Eliminación
- IM: Minimización del impacto
- CR: Corrección
- RC: Recuperación
- AD: administrativa
- AW: concienciación
- DC: Detección
- MN: Monitorización
- Std: normal
- Proc: Procedimiento
- Cert: Certificación

La siguiente columna hace referencia, como se ha especificado, al nivel de recomendación. Todas aquellas *salvaguardas* que se apliquen a la organización tendrán un número del 1 al 10 para especificar lo necesario que considera Pilar que se apliquen, además de que tendrán la casilla de al lado marcada con un color rojo.

Pasando a los nombres de las *salvaguardas*, es posible ver que tienen un paraguas con diferentes colores. Un color gris significa que su peso es bastante bajo, pero que aun así es interesante y se podría estudiar. Un color verde significa que es una *salvaguarda* importante y que podría resultar en la mejora de la seguridad de la organización. Un color amarillo significa que la medida es necesaria y se debería de implementar en un corto plazo. Un color rojo significa que la medida es crítica y que debe ser implantado lo antes posible para reducir los riesgos a los que la empresa se enfrenta.

Por último, es interesante conocer los niveles que establece el ENS en la última columna. Estos niveles hacen referencia a la madurez de las medidas de protección, y

muestra el nivel de madurez que se alcanzaría si se implantara las *salvaguardas* sugeridas.

- n.a: Como ya se ha explicado, esto hace referencia a que la *salvaguarda* en cuestión no se aplica, es como si no existiera.
- L1: En este caso se considera que hay un pequeño esfuerzo, crear esta *salvaguarda*, pero todavía no se ha desarrollado su aplicación en la organización o todavía está en una fase de maduración temprana.
- L2: La *salvaguarda* ya está siendo aplicada, pero no hay ningún protocolo de uso y realmente se utiliza gracias a la gestión de los responsables.
- L3: La *salvaguarda* ha sido implementada y tiene protocolos de uso
- L4: La *salvaguarda*, además de lo establecido por el L3, tiene mecanismos que miden su funcionalidad y su eficacia para asegurarse de su profesionalidad.
- L5: La *salvaguarda*, además de lo establecido anteriormente, dispone de mecanismo de mejora que permiten, usando los medidores del nivel anterior, mejorarla para que su uso sea lo más eficiente y profesional posible.

Anexo II. Registro de Actividades de Tratamiento del Organismo (RAT).

En el presente anexo, se muestra una BBDD en SQLSERVER para contener todos los datos necesarios con el objeto de gestionar el registro público, que contiene los tratamientos con todos los datos obligados por el RGPD. Se acompaña de un script SQL de creación de la base de datos en una instancia (INSTANCIA) de SQLSERVER.[3]

En el TFG actual no se ha implementado la aplicación de registro, únicamente las tablas, sus relaciones y los procedimientos almacenados en la Base de Datos, por la amplitud del tema a desarrollar. Queda, para posteriores TFG, el diseño de la aplicación que gestione el RAT.

[3] Base de datos RAT (google drive)

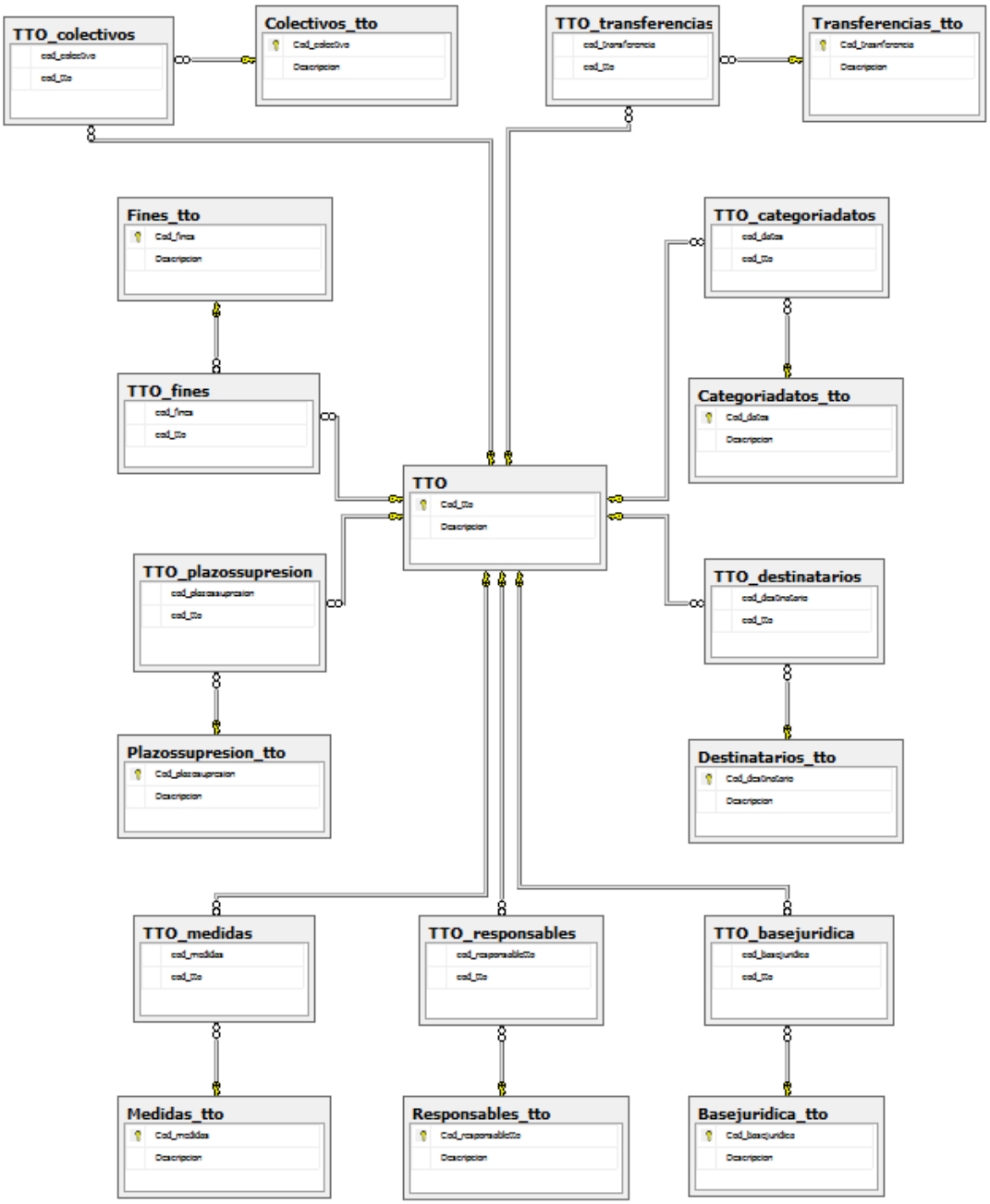


Diagrama de Base de Datos RAT.

ANEXO ODS

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				x
ODS 2. **Hambre cero.**				x
ODS 3. **Salud y bienestar.**				x
ODS 4. **Educación de calidad.**				x
ODS 5. **Igualdad de género.**				x
ODS 6. **Agua limpia y saneamiento.**				x
ODS 7. **Energía asequible y no contaminante.**				x
ODS 8. **Trabajo decente y crecimiento económico.**			x	
ODS 9. **Industria, innovación e infraestructuras.**				x
ODS 10. **Reducción de las desigualdades**.	x			
ODS 11. **Ciudades y comunidades sostenibles**.				x
ODS 12. **Producción y consumo responsables.**		x		
ODS 13. **Acción por el clima.**				x
ODS 14. **Vida submarina.**				x
ODS 15. **Vida de ecosistemas terrestres.**				x
ODS 16. **Paz, justicia e instituciones sólidas.**	x			
ODS 17. **Alianzas para lograr objetivos.**		x		

Reflexión sobre la relación del TFG con los ODS y con los ODS más relacionados.

El TFG se ha realizado con el propósito de hacer más sencillo, a las figuras responsables de los tratamientos de datos personales. el cumplimiento del RGPD, el ENS y la LOPDGDD en las AAPP. También se han proporcionado una serie de medidas, salvaguardas o controles que facilitan la transición al nuevo Esquema Nacional de Seguridad de reciente publicación. Por lo tanto, el objetivo de este TFG no deja de ser el de crear unos **organismos sólidos** en la Protección de los Datos Personales de personas físicas. De igual forma, también se busca garantizar que las personas puedan ejercer sus Derechos recogidos en el RGPD y en la LOPDGDD, que permiten asegurar los Derechos y Libertades fundamentales recogidas en la Constitución.

Otro objetivo con el que está comprometido este TFG es el de **acabar con las desigualdades**, pues gran parte de los riesgos a los que se ven expuestos los datos al no seguir la normativa de seguridad o no llevar a cabo una correcta evaluación de riesgos está relacionada con amenazas de desigualdad social (por ejemplo, discriminación). En el TFG se presentan una serie de medidas de protección que buscan, ya no sólo eliminar la posible amenaza, sino también contribuir a la resolución de incidentes, que, en caso de producirse, provocarían unos perjuicios muy serios a las personas físicas y a la reputación de la organización.

El objetivo final del ENS es proteger a las Administraciones Públicas para que no sen objeto de ataques y garantizar en todo momento las características de la seguridad. A este fin contribuyen varios organismos. Para empezar, el CCN, que es el encargado de velar y guiar en la aplicación del ENS, de ahí sus guías de seguridad y buenas prácticas. El organismo de control que obliga el RGPD en España es la AEPD y las agencias autorizadas autonómicas. No sólo se aseguran de velar por la seguridad de los sistemas de información, sino que además buscan la concienciación de las empresas y organismos públicos. Además, para la implantación de las medidas descritas hace falta **coordinación entre los diferentes departamentos** y concienciación sobre la necesidad de proteger los datos que se tratan.

Todos estos datos son tratados y transferidos a diario, considerados como recurso (al igual que si fuera dinero o bienes materiales) que se debe aprovechar, ya sea para vender mejor los productos o para poder realizar proyectos estadísticos. Realizar una evaluación de riesgos y su posible impacto puede ayudar a fomentar un **consumo responsable**, así como evitar fugas de información y posible robo de datos por parte de terceros.

En una menor medida, se podría decir que este TFG también ayuda al **trabajo decente y crecimiento económico** ya que, si se consiguen cumplir en todas las dimensiones de seguridad, el valor de las instituciones subirá y genera una confianza hacia la ciudadanía que redundará en el uso de sus servicios. No sólo las instituciones, sino también las entidades privadas que dan servicios para el Servicio Público.

En resumen, se considera que este TFG trata algunos de los objetivos para lograr un futuro más sostenible y comprometido con la sociedad según las ODS aprobadas por la ONU en 2015.